

***United States Department of Agriculture (USDA)
eGovernment Program***

eAuthentication Integration Guidebook

May 20, 2004





Table of Contents

1	Introduction.....	1
1.1	Purpose.....	2
1.2	Audience	2
1.3	Scope.....	2
1.3.1	In Scope	2
1.3.2	Out of Scope	2
2	eAuthentication Overview	3
2.1	Why eAuthentication	3
2.1.1	Freedom to E-File Act of 2000	3
2.1.2	Government Paperwork Elimination Act of 1998	3
2.1.3	Our technology and the rest of the Federal Government.....	4
2.2	eAuthentication High-Level Functionality	5
2.2.1	Security Services.....	5
2.2.2	Assurance Levels	6
2.2.3	Registration.....	6
2.2.4	Application-Specific Permissions.....	8
2.2.5	User Management.....	8
2.2.6	User Information.....	9
2.3	eAuthentication System Architecture	10
2.3.1	Technology Used	10
2.3.2	How the Technology Works	10
2.4	Additional Services Offered by eAuthentication.....	12
2.4.1	Project Planning and Strategy.....	12
2.4.2	Integrated Application Support.....	12
2.4.3	Development.....	12
2.4.4	Infrastructure.....	13
2.4.5	Help Desk.....	13
3	eAuthentication Online Functionality.....	14
3.1	Navigation Bar Buttons.....	14
3.2	Quick Links and Employee Links.....	14
3.3	Pages Common to All Users.....	15
3.3.1	eAuthentication Home page.....	15
3.3.2	About eAuthentication page	16
3.3.3	Help page	17
3.3.4	Contact Us page	18
3.3.5	FAQ page.....	19
3.3.6	What is an Account? page.....	20
3.3.7	Log-In Warning! page.....	21
3.3.8	USDA Web Services Log-In page.....	22
3.3.9	eAuthentication Status page.....	23
3.3.10	Logoff pages	26
3.4	Account Registration	27
3.4.1	Create Account page.....	27



- 3.4.2 Create an Account Level 1..... 28
- 3.4.3 Account Creation Confirmation Email 31
- 3.4.4 Account Activation page..... 32
- 3.4.5 Create an Account Level 2..... 33
- 3.4.6 Account Creation Confirmation Email 36
- 3.5 Account Management 37
 - 3.5.1 IMS page..... 37
 - 3.5.2 Modify my Profile – Level 1 page..... 38
 - 3.5.3 Modify my Profile – Level 2 page..... 39
 - 3.5.4 Apply for Level 2 Authentication page 40
 - 3.5.5 View my Roles page 41
 - 3.5.6 Change My Password page..... 42
- 3.6 Password Maintenance..... 43
 - 3.6.1 Change Password page 43
 - 3.6.2 Forgotten Password Recovery for Level 1 users 44
 - 3.6.3 Forgotten Password Recovery for Level 2 users 46
- 3.7 Administrative Accounts 48
 - 3.7.1 Local Registration Authority 48
 - 3.7.2 Validate Level 2 Customer: Search for Level 2 Customer 49
 - 3.7.3 Search Results in Organization page 50
 - 3.7.4 Validate Level 2 Customer page..... 51
 - 3.7.5 Application Administrator 52
 - 3.7.6 Grant User Access Role: Search for a Role Admin User page..... 53
 - 3.7.7 Grant User Access Roles page..... 54
- 4 Integration..... 56
 - 4.1 Integration Overview 56
 - 4.2 Pre-Integration 57
 - 4.2.1 Form an Application Team 57
 - 4.2.2 Integrated Reporting - Identify the Interactions in the Application..... 57
 - 4.2.3 Design and Implement Application 58
 - 4.2.4 Review eAuthentication Guidebook..... 58
 - 4.2.5 Set up Pre-Design meeting with eAuthentication Integration team..... 59
 - 4.3 Pre-Design Meeting 60
 - 4.3.1 Facilities Needed for the Pre-Design 60
 - 4.3.2 Introductions to the Integration team..... 60
 - 4.3.3 eAuthentication Overview 61
 - 4.3.4 eAuthentication Demonstration 61
 - 4.3.5 Introduce the Application Integration Form 61
 - 4.4 Design Meeting(s)..... 62
 - 4.4.1 Choose Hosting Environment(s)..... 62
 - 4.4.2 Determine Application Permission Needs 64
 - 4.4.3 Determine Authorization Needs 66
 - 4.4.4 Design the Mapping Process Application Users to the eAuthentication
Common Data Store..... 67



- 4.4.5 Design Logoff page..... 67
- 4.5 Funding 69
 - 4.5.1 How is funding determined?..... 69
 - 4.5.2 Who makes the decision?..... 69
- 4.6 Build..... 70
 - 4.6.1 Network Connectivity between the Policy Server and the Web Agent 70
 - 4.6.2 Install Web Agents..... 71
 - 4.6.3 Configure Integration..... 71
 - 4.6.4 Understanding and Capturing Header Variables 71
 - 4.6.5 Build Data Mapping Page(s)..... 77
 - 4.6.6 Build Logoff Page..... 78
 - 4.6.7 Test Integration 78
 - 4.6.8 Migrate to Production 79
- 4.7 Registration Certification..... 80
- 5 Detailed Development Information 81
 - 5.1 Password Policies..... 81
 - 5.1.1 Password Policy Level One 81
 - 5.1.2 Password Policy Level Two..... 81
 - 5.1.3 Force Change Password..... 81
 - 5.2 Account Policies/Session Management 82
 - 5.2.1 Account Expiration 82
 - 5.2.2 Account Lockout..... 82
 - 5.2.3 Maximum Timeout 82
 - 5.2.4 Idle Timeout..... 82
 - 5.3 Netegrity SiteMinder References..... 83
 - 5.3.1 Realms..... 83
 - 5.3.2 Rules 83
 - 5.3.3 Responses..... 83
 - 5.4 eAuthentication Platform Support 85



1 Introduction

Through legislated mandate, the United States Department of Agriculture (USDA), where practicable, must provide electronic alternatives to traditional paper-based processes including accepting electronic rather than manual signatures. The three principal acts relevant to this policy are: Government Paperwork Elimination Act (GPEA); Electronic Signatures in Global and National Commerce Act (E-Sign); and Freedom to E-File Act.

To enable the secure presentation of information and to enable electronic signature of submissions, the USDA has developed a centralized eAuthentication solution to provide authentication services for online applications. Managed by the USDA Office of the Chief Information Officer (OCIO), eAuthentication is an enabling process and technological foundation that will help USDA achieve its goals and objectives for eGovernment by supporting all USDA eGovernment initiatives and applications.

The USDA eAuthentication solution serves as the centralized authentication service for USDA web services, relieving applications of the need to build and maintain their own authentication services. USDA eAuthentication also provides centralized administration of users. In addition, eAuthentication provides a unified credential that can be used to provide users with single sign-on capability across all participating web applications. Single Sign-on allows an authenticated user (a user that has logged in with proper credentials) to move seamlessly between participating USDA applications. Each time the user accesses a different application, eAuthentication checks that the user has the proper authorization and grants or denies access accordingly.

In addition to providing the user with a single sign-on experience at all USDA sites, eAuthentication will accommodate the General Services Administration (GSA) “federated” architecture. This “federated” architecture design allows participating agency applications and credential services to communicate directly through standards, specified by industry in an effort to provide Single Sign On across the Federal government. By accommodating these standards, eAuthentication has the potential to provide authentication and credential services other Presidential eGovernment Initiatives. Additionally, eAuthentication will accept the credentials issued by other Government Departments.



1.1 Purpose

The purpose of this document is to provide a detailed description of eAuthentication system architecture, functionality, technologies, as well as the process and development information needed to integrate an application with the USDA eAuthentication solution.

Section 2: eAuthentication Overview and Section 3: eAuthentication Online Functionality both provide an overview and high-level description of the eAuthentication service. Section 4: Integration and Section 5: Detailed Development Information both provide more detailed information regarding integration and agency-specific requirements.

1.2 Audience

This document is intended to provide guidance for agency Application Business Owners and Development team members who will be making decisions for new USDA agency applications.

Application owners should read this document if their application requires eAuthentication. eAuthentication is required for all USDA, web-based applications with a primary user base consisting of customers, employees, and/or affiliates that require their identity to be established by a User ID. eAuthentication is not required for mainframe or client-server based systems, nor is it required for LAN networks. For more information, please refer to Section 2.1: Why eAuthentication.

1.3 Scope

1.3.1 In Scope

This document will provide a step-by-step guidance for an agency to understand and make prudent decisions, and implement a secure architecture for online applications. This document will discuss authentication, application permissions, authorization, application integration, hosting and registration procedures that will ensure the integrity of confidential information being transferred over the Web.

1.3.2 Out of Scope

This document does not constitute an agreement of services nor does it include all of the specifics of the eAuthentication architecture.

2 eAuthentication Overview

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. The eAuthentication initiative aims to provide a single, centralized authentication service for web-based authentication of individuals throughout the Department. This service provides for the identification and validation of USDA's customers before they are allowed access into participating USDA web-based systems. The eAuthentication service provides a single credential (currently a password, other credentials may be available in the future) that a USDA web user can present to any participating USDA web site. This credential is defined as a proof of user identity; the user must enter this proof only once in the form of a username and password when first trying to log into a protected site. As a result, the eAuthentication service reduces the burden on customers to register for, and maintain, separate online identities with each of the numerous online systems.

2.1 Why eAuthentication

eAuthentication is a part of the eGovernment initiative, one of several programs outlined in the Presidential Management Agenda (other initiatives include Strategic Management of Human Capital, Competitive Sourcing, Improved Financial Performance, and Budget and Performance Integration). The eAuthentication service resulted from two legislative mandates designed for eGovernment: The Freedom to E-File Act, and the Government Paperwork Elimination Act (GPEA).

2.1.1 Freedom to E-File Act of 2000

To the maximum extent practicable, this act establishes an Internet-based system that enables agricultural producers to access all forms of the agencies of the Department of Agriculture.

2.1.2 Government Paperwork Elimination Act of 1998

The Government Paperwork Elimination Act (GPEA) required agencies, by October 21, 2003, to provide an electronic option for maintenance, submission, or disclosure of information, when practicable as a substitute for paper. GPEA also entails the use and acceptance of electronic signatures, when practicable.



2.1.3 Our technology and the rest of the Federal Government

2.1.3.1 General Services Administration (GSA)

eAuthentication is working closely with the General Services Administration (GSA) effort to create an architecture design to allow participating agency applications and credential services to communicate directly through standards specified by the industry. GSA has formed an Architecture Working Group (AWG) composed of its own personnel and representatives from key participating agencies, including USDA.

2.1.3.2 WebCAAF Vs. eAuthentication

WebCAAF, or the Web-based Centralized Authentication and Authorization Facility, was built by the Service Center agencies in 2001 and forms the core of the eAuthentication service. The larger eAuthentication service provides the functionality originally provided by WebCAAF, as well as user management improvements, expansions to serve all other agencies, and standardization to integrate with the Federal e-Authentication initiatives. In addition, eAuthentication includes other ongoing initiatives to increase the scope of credential types and audience types for USDA web-based authentication.

2.1.3.3 USDA eAuthentication Vs. GSA E-Authentication

The presidential eAuthentication and the USDA eAuthentication systems are related, but some clarification is given here on the difference. The presidential eAuthentication service performs authentication services across all of the governmental departments. This includes the USDA, the National Institute of Science & Technology, and the United States Patent Office.

USDA eAuthentication is an effort applicable specifically across all USDA agencies. This document deals only with USDA eAuthentication.

2.1.3.4 Integration History

The eAuthentication project went live on October 19, 2003 supporting 48 applications. The eAuthentication project is supported by a series of groups that ensure infrastructure maintenance, applications integrations, and project planning. For more information, please refer to Section 2.4: [Additional Services Offered by eAuthentication](#). As of 1/29/2004, the USDA eAuthentication Service supports over 30 customer facing applications, and 26 additional applications are scheduled to be integrated.

Agency applications wishing to integrate with the eAuthentication service should first read this guidebook and then contact the eGovernment program to schedule an eAuthentication Pre-Design meeting.



2.2 eAuthentication High-Level Functionality

2.2.1 Security Services

The eAuthentication system provides authentication and application permissions, as well as user information, to the application for authorization purposes. These services are provided on a per-URL basis and can be applied to either the whole site/application or to individual pages and folders, as long as they are differentiated by URL.

2.2.1.1 Authentication

Authentication is the process of identifying the user based on their login name and knowledge of a shared secret (password). A user will not be granted access to any protected application unless he has successfully authenticated.

2.2.1.2 Application Permissions

Application Permissions are the criteria used to further restrict access to the application after the user has been authenticated. Application Permissions determine which types of users have access to particular resources. Each application owner is responsible for determining the business rules that determine application permissions. eAuthentication is responsible for implementing these rules.

Implementation of Application Permissions is done through an automated process using criteria specified by each application's needs. Users can be restricted based on what level of assurance they currently have, or based on user "common data." Of the numerous available user attributes, one is user location. For example, eAuthentication can be configured so that only users from the state of Montana can access a certain site where users from all other states are not allowed to access the site (even if they enter a valid username and password).

2.2.1.3 Role-Based Application Permissions

Application Permissions can also be role-based. Roles are characteristics, functions, or positions for an individual. Roles are created by the Application Owner, and users are assigned roles by these application administrators. Independent of assurance level and other permissions, the role-based application permissions simply confirms that a user has been assigned a certain role before allowing the user to access the protected site. For more information, please refer to Section 4.4.2: Determine Application Permission Needs.

2.2.1.4 Authorization

Authorization is a process independent of Authentication and the use of Application Permissions. Authorization defines what a user is allowed to do once inside the agency application. For example, a user is assigned a particular job in the application database,



so that say a farmer is allowed to submit a loan request, but only a bank administrator is allowed to approve it.

Authorization involves giving a user permission to access a certain resource (i.e., application or web site). When a user attempts to access a resource, the system checks the user's account to see if their permissions match the allowed attributes. The application may choose to rely on information passed through header variables to make authorization decisions. However, eAuthentication does not implement authorization decisions.

2.2.2 Assurance Levels

Assurance is defined as how much confidence the relying party has that the electronic identity credential presented is done so by the person whose identity is asserted by the credential.

The Office of Management and Budget has established guidelines that establish four levels of assurance. Each assurance level describes the agency's degree of certainty that the user has a credential. A credential is defined as an object that is verified when presented to the verifier in an authentication transaction.

- **Level 1 Assurance** – Little or no confidence in the asserted identity's validity. Credentials with level 1 assurance require a username and password.
- **Level 2 Assurance** – Some confidence in the asserted identity's value. Credentials with level 2 assurance require a username and password; the user must be identity-proofed by a designated Local Registration Authority (LRA).
- **Level 3 Assurance** – High confidence in the asserted identity's validity – eAuthentication does not currently support Level 3.
- **Level 4 Assurance** – Very High Confidence in the asserted identity's validity – eAuthentication does not currently support Level 4.

Determination of which level of assurance is required is at the discretion of the resource owner, following OMB guidelines.

2.2.3 Registration

Registration is the process by which new users request access to the system by obtaining a user name and password. In addition to choosing a user name and password, the process requires new users to provide information about themselves. eAuthentication currently accommodates registration procedures for both Level 1 and Level 2. Depending on the level for which the user is applying, different amounts of information must be entered.



As Level 2 applicants, users must provide enough information to facilitate in-person identification (i.e., address and date of birth).

2.2.3.1 Level 1 Registration

Level 1 Registration requires a limited amount of information to complete customer user profile. It requires a minimum 4 character password and does not utilize any identity proofing. After a user registers, they receive an email confirmation to activate their customer profile with Level 1 credentials

Level 1 credentials are typically used for customization or to ensure the availability of contact information (e.g. a valid email address). For more information, please refer to [Section 3.7.5: Application Administrator](#).

2.2.3.2 Level 2 Registration

Level 2 Registration requires a user to complete an expanded user profile. It requires a minimum 9 character password and authentication of identity by a USDA employee. After a user registers, they receive email confirmation to activate their customer profile with Level 2 credentials. The account is initially assigned only assurance of Level 1. Only after the user is validated by an LRA is their account upgraded to a level 2 assurance.

The eAuthentication team and the USDA Service Centers provide a default user registration process consisting of user self-registration and in-person “identity-proofing” at the USDA Service Centers. User passwords will be enabled for Level 2 authentication once a user’s identity has been confirmed by the Service Center Local Registration Authority (LRA).

An agency may also choose to provide LRA services outside of the service centers, but must work with the eAuthentication Integration team to create and approve these procedures. LRA identity-proofing procedures can be certified by scheduling a Certification meeting with the eAuthentication team. For more information, please refer to [Section 4.7: Registration Certification](#) and [Section 2.2.5: User Management](#).

It is the responsibility of a local registration authority (LRA) to match the customer’s identification credentials to the information stored in the eAuthentication database, thereby verifying the identity of the customer. Once this is complete, a user can successfully become a Level 2 user. For more information, please refer to [Section 4.7: Registration Certification](#).

2.2.3.3 Upgrade Level 1 User to Level 2

An upgrade from Level 1 to Level 2 requires additional customer information in the expanded user profile. It requires verification of identity by a USDA employee. After a



user registers, they will receive a confirmation email, but no additional activation is required.

It is the responsibility of a local registration authority (LRA) to match the customer's identification credentials to the information stored in the eAuthentication database thereby verifying the identity of the customer. Once this is complete, a user can successfully become a Level 2 user. For more information, please refer to Section 4.7 Registration Certification.

2.2.4 Application-Specific Permissions

Permissions are assigned to users by Application Administrators. Application Administrators are users that have the authority to assign one or more sets of permissions to users. If role-based application permissions are used to protect an application, Application Administrators can assign users the required Application Permission roles.

If, for example, only representatives of utility companies are allowed to access a particular online form, Application Permissions will be enforced by creating a role called "UTILITY_CO_ROLE." Application owners would designate a user to become an Application Administrator. This Application Administrator confirms that the user is a representative of the utility company and then assigns them the "UTILITY_CO_ROLE" appropriate role.

The integration team can make any user with level 2 assurance or higher an Application Administrator based upon an application owner's request. Application owners can only request that their Application Administrators have the right to assign roles that relate to their application. To do this the agency application owner(s) must provide the name and User ID of those users which will become Application Administrators. For more information, please refer to Section 3.5.5: View my Roles page and Section 3.7.5: Application Administrator.

2.2.5 User Management

Once a user account has been created using the above registration methods, the user can access and update their account by logging in to eAuthentication. For more information, please refer to Section 3.5: Account Management.

User Management includes:

- **Modify My Profile** – This function allows a user to change the user attributes stored in their eAuthentication user account.



- **Apply for Level 2 Authentication** – This function allows level 1 users to enter the information needed to register for level 2 accounts. This function is only displayed for level 1 users.
- **Change My Password** – This function allows users to change their password.
- **View My Permissions** – This function allows users to view the application permissions that they have been assigned by application administrators.

2.2.6 User Information

eAuthentication maintains a repository of common user data (e.g., their user name, first name, last name, address, etc.) that is shared among agencies and applications. It is important to consider that level 1 users have different sets of required attributes than level 2 users. Level 2 users are required to store address information that is not required of level 1 users. For a complete list of required attributes stored for different types of users see [Level 1 Requirements for required Common Data Elements](#) and [Level 2 Requirements Common Data Elements](#).

User data attributes stored by eAuthentication can be passed to applications in the form of header variables at the time that a user accesses an application.

2.2.6.1 User Information

Several default variables are passed on every request by the system. They include user name, realm, and user DN. For more information, please refer to [Section 4.6.4: Understanding and Capturing Header Variables](#) and [Section 5.3.1: Realms](#).

2.2.6.2 Default Header Variables

Several default variables are passed on every request by the system. They include user name, realm, and user DN. For more information, as well as a complete list of default variables, please refer to [Section 4.6.4.1: SiteMinder Default Header Variables](#) and [Section 5.3.1: Realms](#).

2.2.6.3 Optional Header Variables

In addition to the default header variables passed, eAuthentication allows participating agency applications to choose to receive optional header variables. These variables can include assurance level, email, first name, or role name. [For more information, as well as a complete list of header variables, please refer to Section 4.6.4.2: USDA Common Data Header Variables](#)

2.3 eAuthentication System Architecture

2.3.1 Technology Used

The USDA eAuthentication service is built upon the Centralized Authentication and Authorization Facility (WebCAAF), technology infrastructure. Technology used for the system includes:

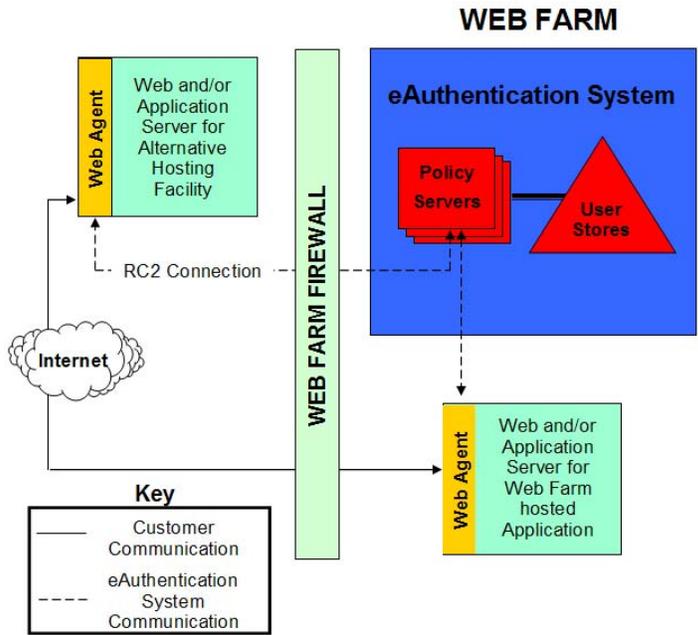
- Netegrity SiteMinder 5.5
- Netegrity IdentityMinder
- Microsoft Active Directory
- 7 WebLogic application servers
- 53 total servers – Development, Pre-production, Production
- Ft. Collins Webfarm Data Center Hosting
- St. Louis Webfarm Data Center Failover

2.3.2 How the Technology Works

The technology making up the eAuthentication system consists of three components:

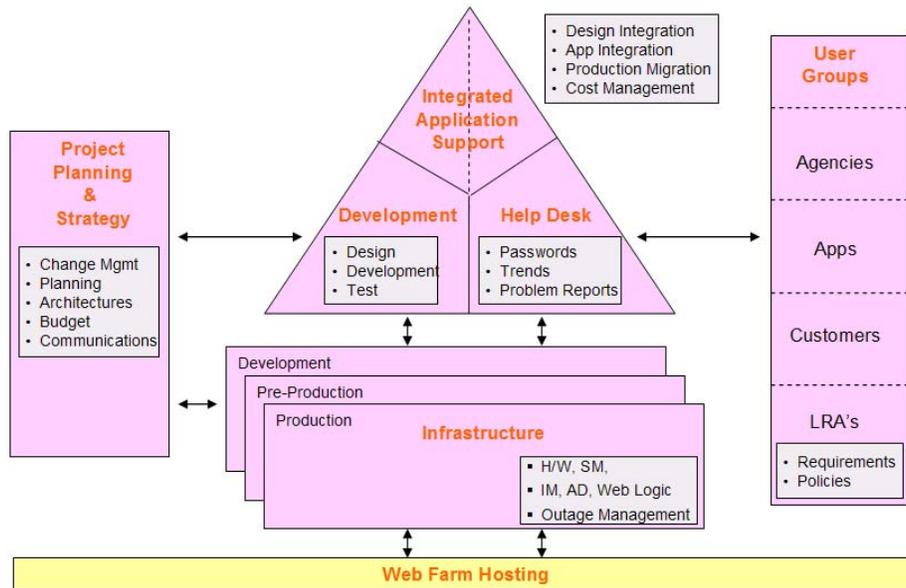
- **User Store** - Central storage of USDA Common Data. Maintains common user information in 1 location that can be utilized by all agencies.
- **Web Agent** - Installed on the agency's web server to perform authentication. Communicates with central authentication system in Web Farm.
- **Policy Server** - Core components of the USDA authentication solution.

A web agent is installed on each protected resource's web server. A web agent intercepts all calls to the protected resource and forwarding the request to the Policy Server. The Policy Server verifies if the user is authenticated into the system; if the user is not, then the user is asked to authenticate against the user store. If the user successfully authenticates using the user store, the policy server then verifies if the user has permissions to access the requested application or web page. If so, the policy server returns the control to the web agent, which allows the user to access the application or web page they have requested.



- ❑ **Policy Server** – Core component of the USDA authentication solution. Ties together web agents and user stores through *Policies*.
- ❑ **User Stores** – Central storage of USDA Common Data. Maintains common user information in 1 location that can be utilized by all agencies.
- ❑ **Web Agent** – Software installed on an application’s web server to help perform authentication. Communicates with eAuthentication Policy Server in Web Farm.

2.4 Additional Services Offered by eAuthentication



2.4.1 Project Planning and Strategy

The project planning and strategy team is responsible for all management tasks of eAuthentication such as establishing a budget, communication of team activities, and planning new tasks for the project. The project manager is also responsible for interfacing with the agencies with regards to integration costs.

2.4.2 Integrated Application Support

The integrated application support team is responsible for designing and implementing the integration process for new applications that are becoming part of the eAuthentication system. The team is responsible for application integration through the production environment.

2.4.3 Development

The development team is responsible for developing and testing upgrades to the system. The team is also responsible for new releases of the eAuthentication environment and ensuring that new releases do not affect current functionalities and requirements.



2.4.4 Infrastructure

The infrastructure of the production environment as well as the maintenance of all applications that are integrated with the eAuthentication system is done by the operations team. This team is responsible for ensuring that the protection of applications is functioning correctly and running at all times according to the Service Level Agreement between the agency and the OCIO.

2.4.5 Help Desk

The eAuthentication Service Help Desk includes procedures such as:

- Initial Password
- Reset Password
- Forgotten Password
- LRA Training Roles
- Change Profile Information
- Change of Assurance Level from 1 to 2

The help desk fields both customer and employee inquiries about eAuthentication services or issues. The help desk also diagnoses whether an issue is eAuthentication-related or if it's application-specific, and they then hand the issue off to the appropriate application support staff.

The help desk can be reached by email at eAuthHelpDesk@itc.nrcs.usda.gov.

3 eAuthentication Online Functionality

This section's purpose is to display all eAuthentication screens and available, online functions. Each page overview shows instructions on opening the page, an overview of the page's purpose and a list of functions available on that page.

3.1 Navigation Bar Buttons

The top portion of every page in eAuthentication is the same. It is called the Navigation Bar. All pages have the same buttons available in this Navigation Bar. Rather than explaining each of these buttons for every page throughout this section, they will only be explained once. The Navigation Bar buttons include:

- The **Home** button - If a user clicks the **Home** button, the *eAuthentication Home* page redisplay. For more information, please refer to Section 3.3.1: eAuthentication Home page.
- The **About eAuthentication** button - If a user clicks the **About eAuthentication** button, the *About eAuthentication* page displays. For more information, please refer to Section 3.3.2: About eAuthentication page.
- The **Help** button - If a user clicks the **Help** button, the *Help* page displays. For more information, please refer to Section 3.3.3: Help page.
- The **Contact Us** button - If a user clicks the **Contact Us** button, the *Contact Us* page displays. For more information, please refer to Section 3.3.4: Contact Us page.
- The **Service Centers** button - If a user clicks the **Service Centers** button, the *Office Information Locator* page displays. This page can also be viewed by typing in its direct URL <http://offices.usda.gov>.

3.2 Quick Links and Employee Links

There is a collection of links on the left of every page in eAuthentication. This collection is made up of two groups called Quick Links and Employee Links. Rather than explaining each of these links for every page throughout this section, they will only be explained once. The links include:

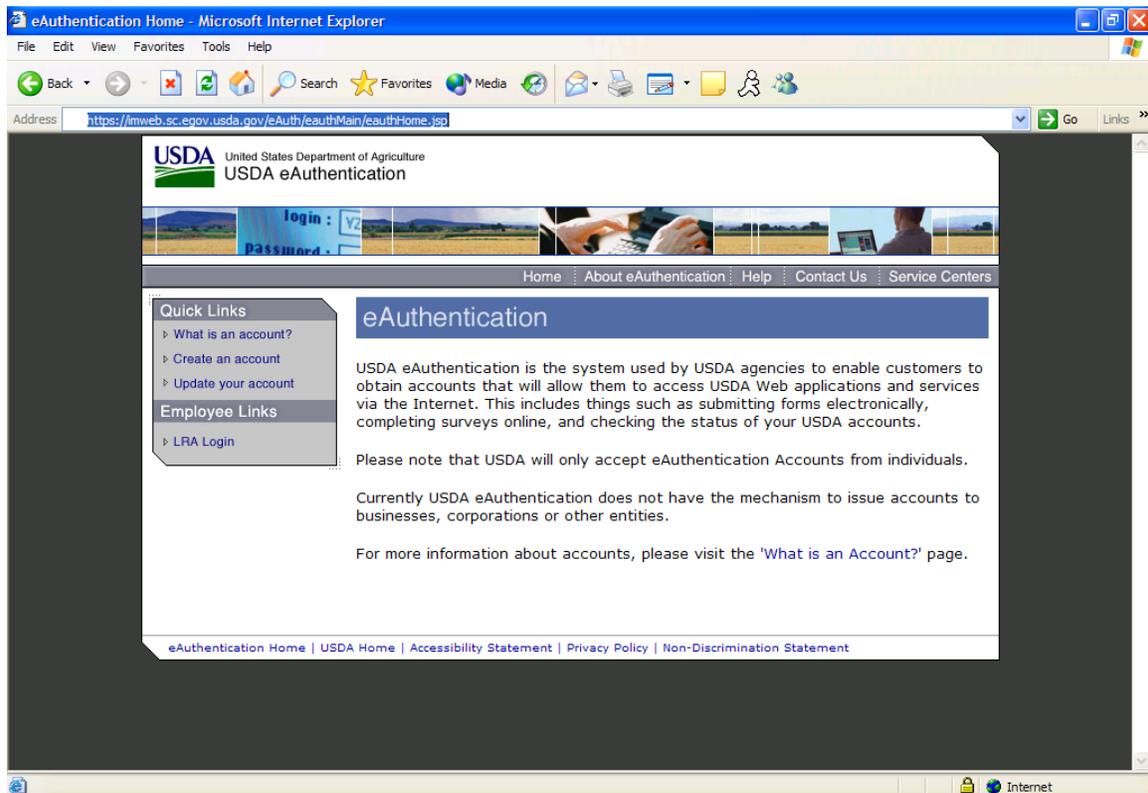
- The **What is an Account** link - If a user clicks the **What is an Account** link, the *What is an Account?* page displays. For more information, please refer to Section 3.3.6: What is an Account? page.

- The **Create an Account** link - If a user clicks the **Create an Account** link, the *Create Account* page displays. For more information, please refer to Section 3.4.1: Create Account page.
- The **Update Your Account** link - If a user clicks the **Update Your Account** link, the user is able to log-in and update their account. For more information, please refer to Section 3.5: Account Management.
- The **LRA Login** link - If a user clicks the **LRA Login** link, the user is sent to an LRA site, where they are able to receive LRA Training or log in as an LRA. For more information, please refer to Section 4.7: Registration Certification.

3.3 Pages Common to All Users

3.3.1 eAuthentication Home page

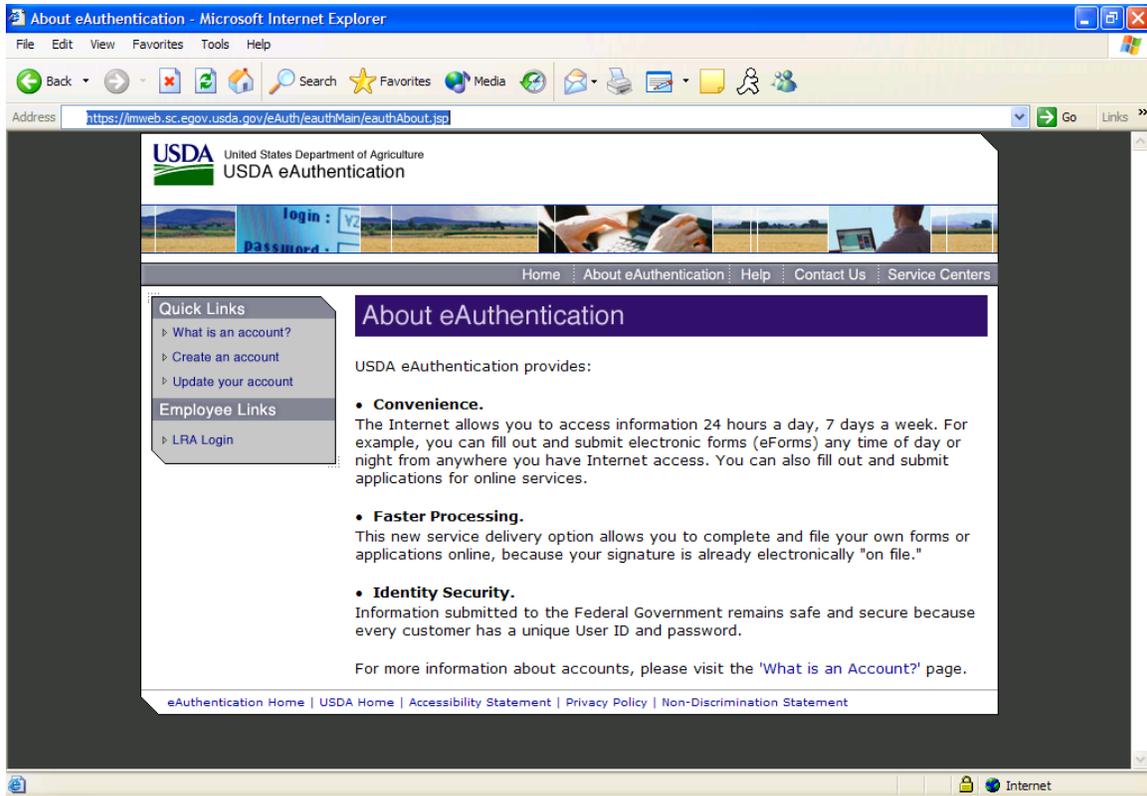
If a user clicks the **Home** button on the top navigation bar the *eAuthentication Home* page displays. This page's address is <http://www.eauth.egov.usda.gov>.



The *eAuthentication Home* page explains the high level functionality and purpose of eAuthentication.

3.3.2 About eAuthentication page

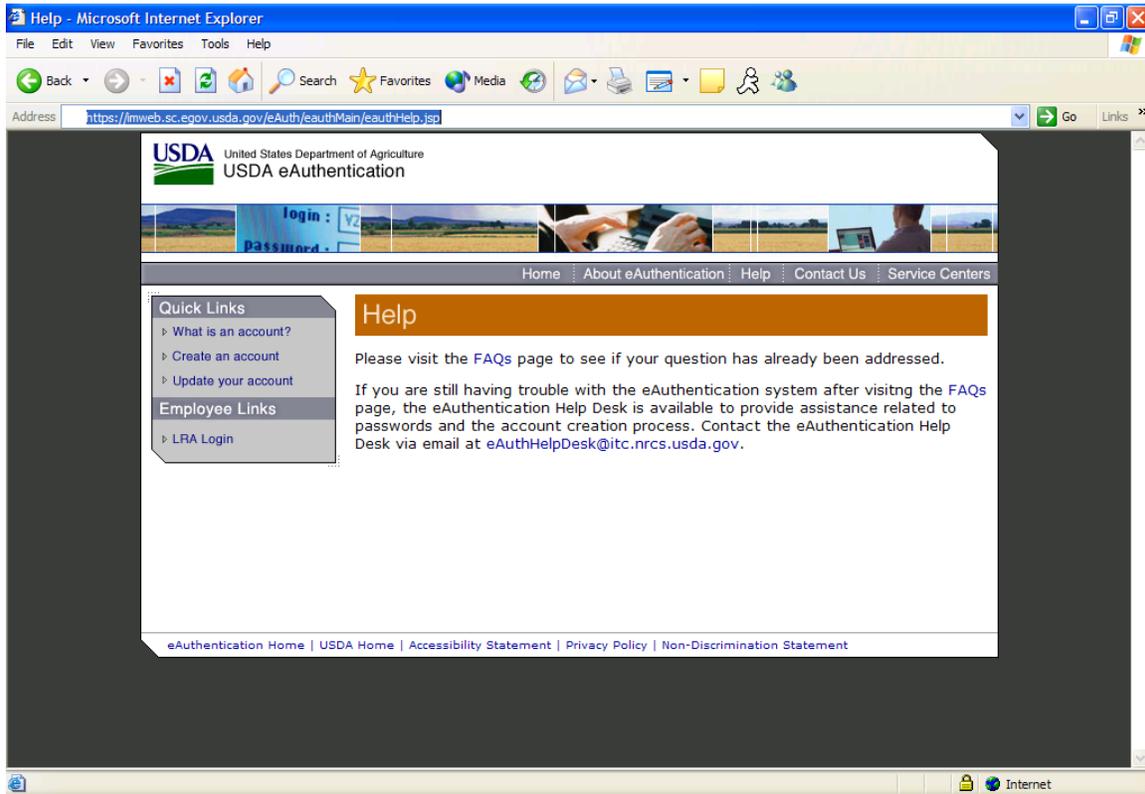
If a user clicks the **About eAuthentication** button on the top navigation bar the *About eAuthentication* page displays. This page's address is <http://www.eauth.gov.usda.gov/eauthAbout.html>.



The *About eAuthentication* page outlines the rationale for and benefits of USDA's choice of eAuthentication. It also describes and contains links for the different identity management options available, including the creation and updating of accounts functionality. It also contains links to the USDA and home page.

3.3.3 Help page

If a user clicks the **Help** button on the top navigation bar the **Help** page displays. This page's address is <http://www.eauth.egov.usda.gov/eauthHelp.html>.

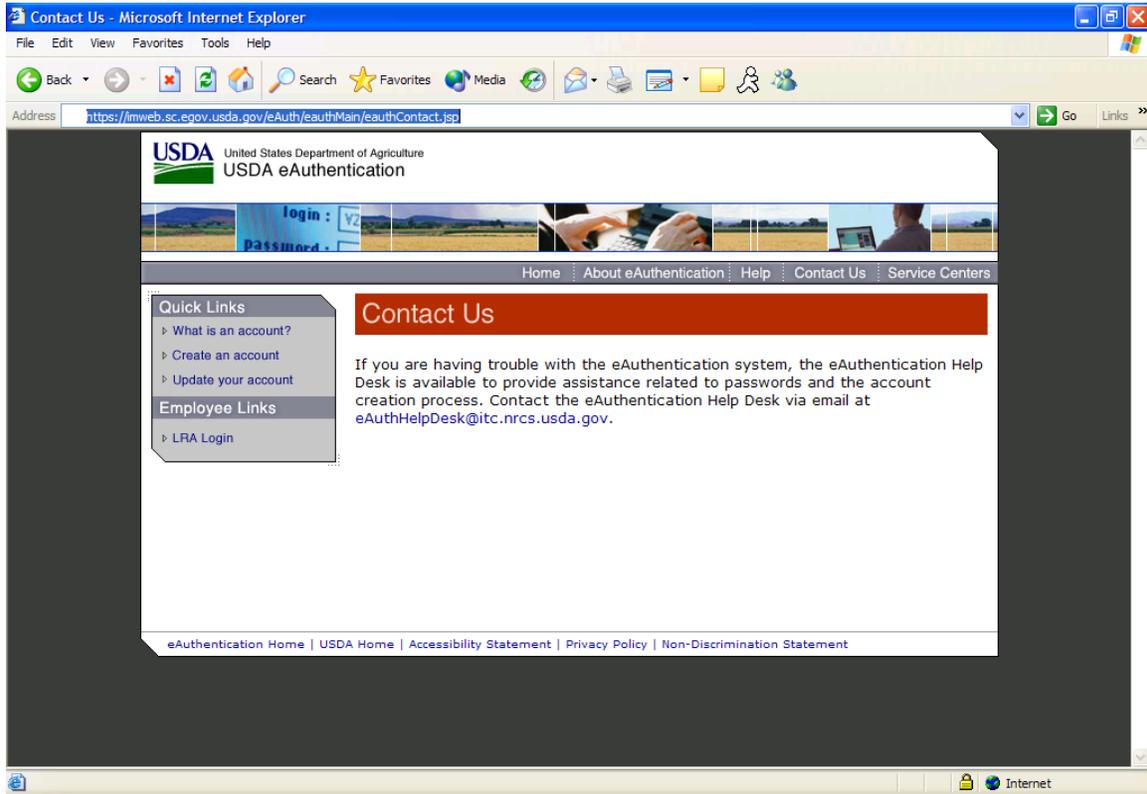


The **Help** page gives users a way to find solutions to any questions or problems they incur while using the eAuthentication system. Included in this list of help solutions are provided a set of Frequently Asked Questions (FAQs) as well as a Help Desk email address.

- If a user clicks the **FAQs** link, the **eAuthentication Help – FAQ** page displays. For more information, please refer to Section 3.3.5: FAQ page.
- If a user clicks the **eAuthHelpDesk@itc.nrcs.usda.gov** link, a new email is created in the user's email program and the "To" section is populated with the above email address.

3.3.4 Contact Us page

If a user clicks the **Contact Us** button on the top navigation bar the *Contact Us* page displays. This page's address is <http://www.eauth.egov.usda.gov/eauthContact.html>.

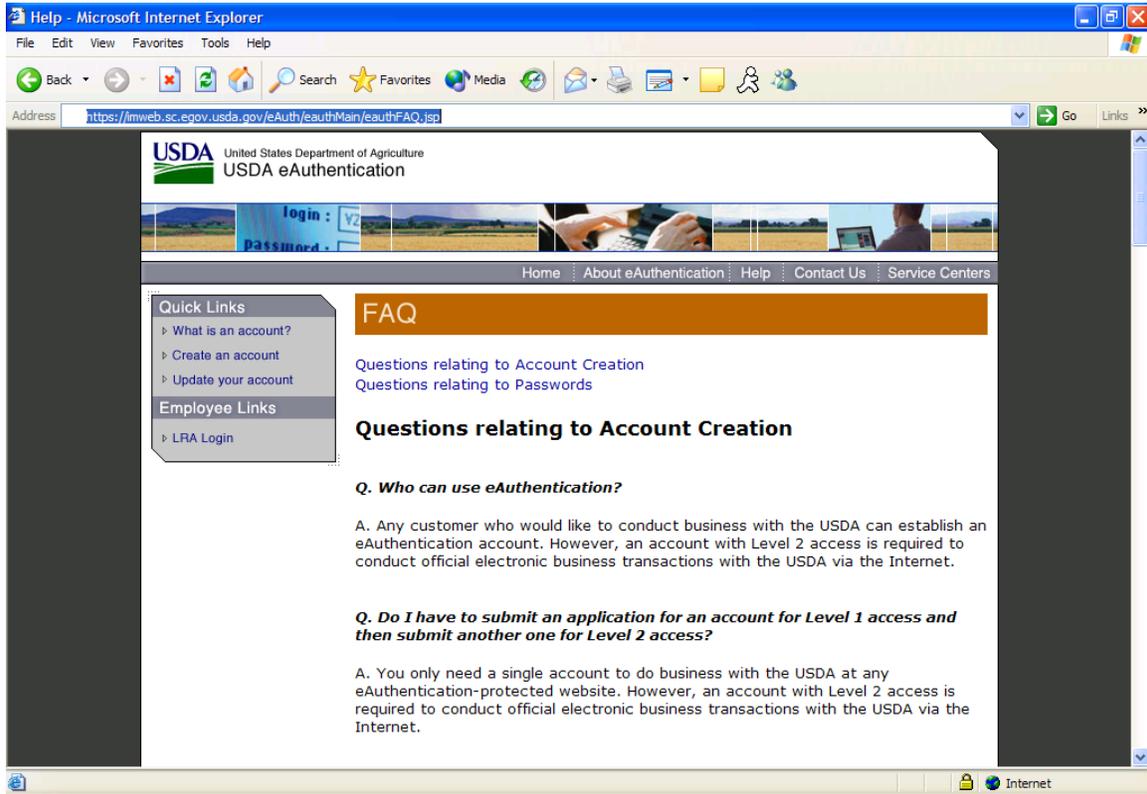


The *eAuthentication Contact Us* page gives users a way to contact a help desk via email.

- If a user clicks the eAuthHelpDesk@itc.nrcs.usda.gov link, a new email is created in the user's email program and the "To" section is populated with the above email address.

3.3.5 FAQ page

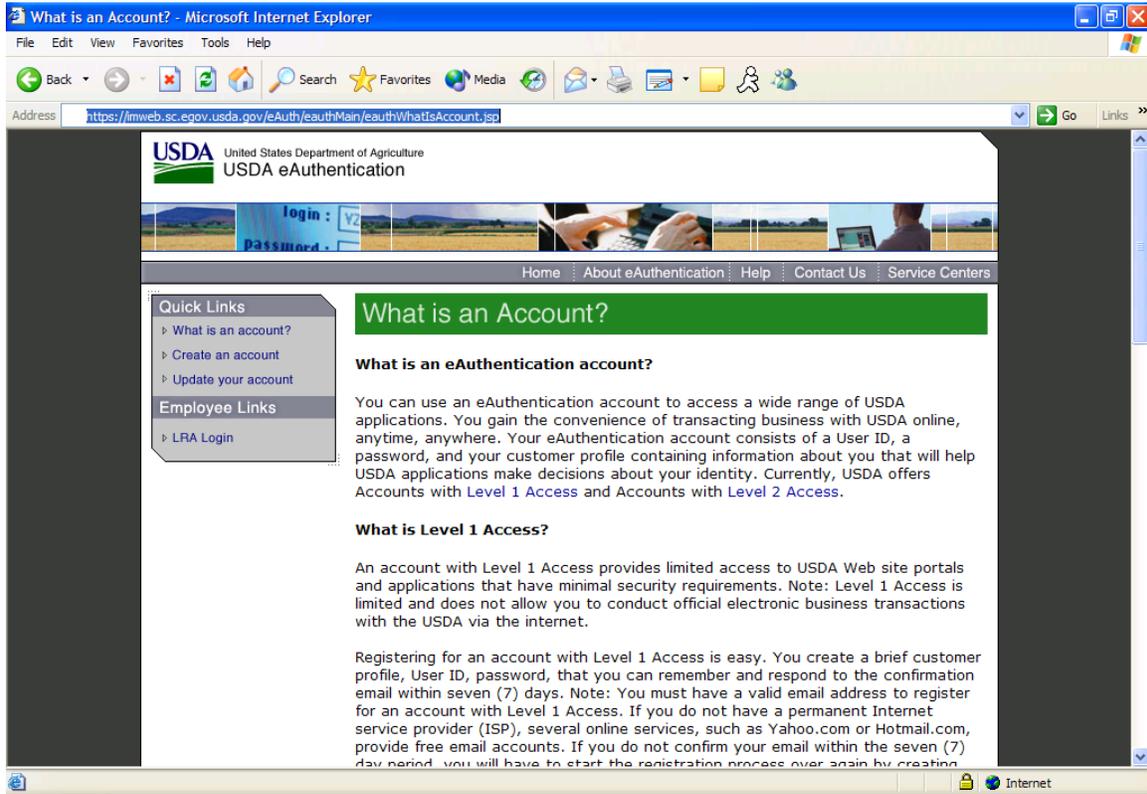
If a user clicks the **FAQs** button on the top navigation bar the **FAQ** page displays. This page's address is <http://www.eauth.egov.usda.gov/eAuthFAQ.html>.



The **FAQ** page answers some common questions that users have. The page is broken into two main sections – one that answers common questions about account creation and another section relating to passwords. The **Questions relating to Account Creation** and **Questions relating to Passwords** links send the user to the appropriate sections of the **FAQ** page.

3.3.6 What is an Account? page

If a user clicks the **What is an account?** link on the top navigation bar the *What is an Account?* page displays. This page's address is <http://www.eauth.egov.usda.gov/eauthWhatIsAccount.html>.

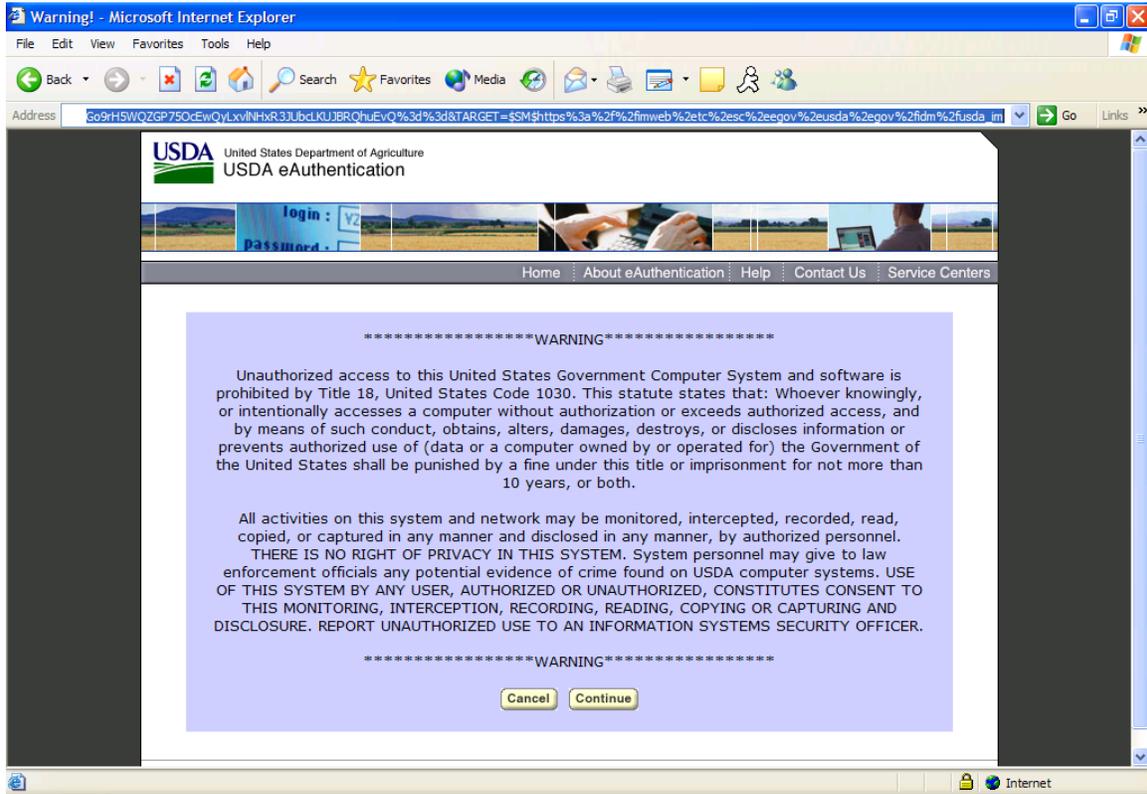


The *What is an Account?* page outlines the definition of the various levels of access. The page is broken into two main sections – one that explains Level 1 access and another that explains Level 2 access.

- If a user clicks the **Create an Account with Level 1 Access** link, the *Create an Account, Level 1* page displays. For more information, please refer to Section 3.4.2: Create an Account Level 1.
- If a user clicks the **Create an Account with Level 2 Access** link, the *Create an Account, Level 2* page displays. For more information, please refer to Section 3.4.5: Create an Account Level 2.
- If a user clicks the **Home** button, the *eAuthentication Home* page displays.

3.3.7 Log-In Warning! page

If a user attempts to access a URL that is protected by eAuthentication (if they enter an address that is protected in the Address field of their browser or click a link that leads to a protected web site) the *Log-In Warning!* page displays.

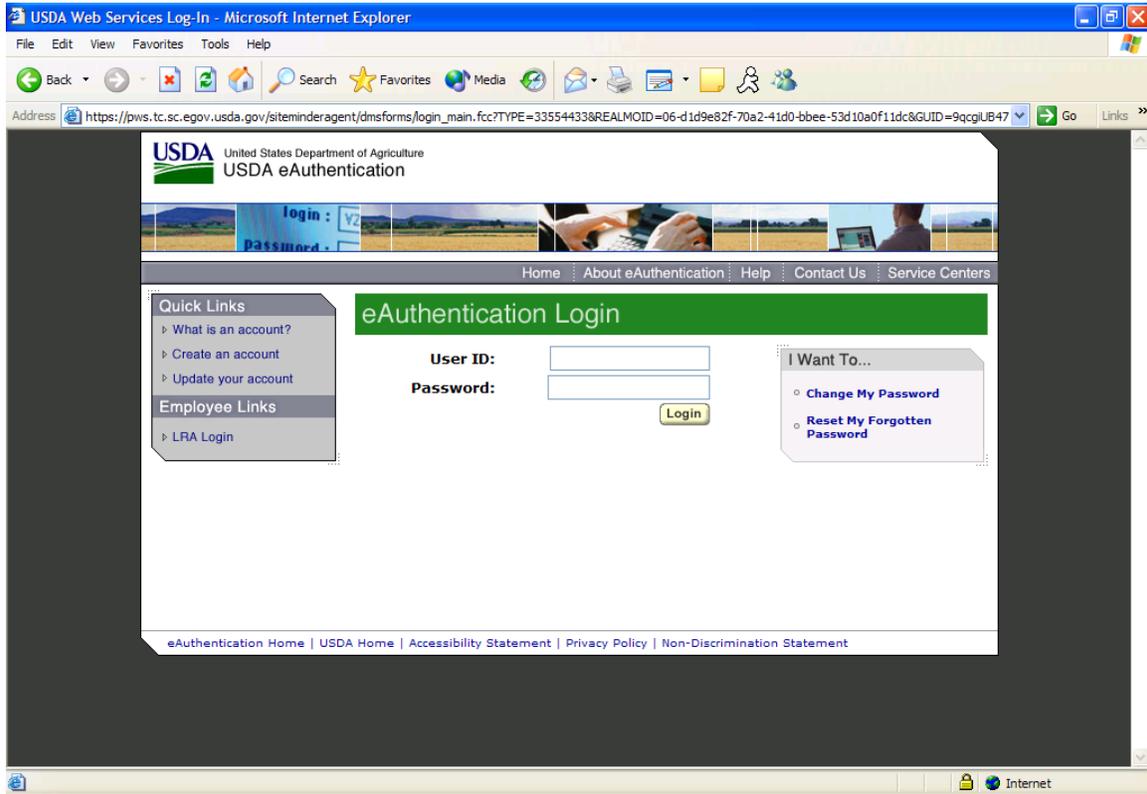


The *Log-In Warning!* page contains a mandatory warning that must be issued to all persons attempting to access an online government application. This warning outlines that unauthorized access is punishable by fine or imprisonment and that those who proceed to access the resources within have no right to privacy.

- If a user clicks the **Continue** link, the *USDA Web Services Log-In* page displays.
- If a user clicks the **Cancel** link, they are redirected to the previous page that was viewed on their browser.

3.3.8 USDA Web Services Log-In page

If a user a user accepts the warning on the *USDA Log-In Warning* page the *USDA Web Services Log-In* page displays.



eAuthentication uses this page to collect credentials for non authenticated users. To log in a user must enter their username in the **User ID** field, their password in the **Password** field, and click the Login button. If the user has the correct application permissions and a valid User ID and Password they are given access to the protected URL.

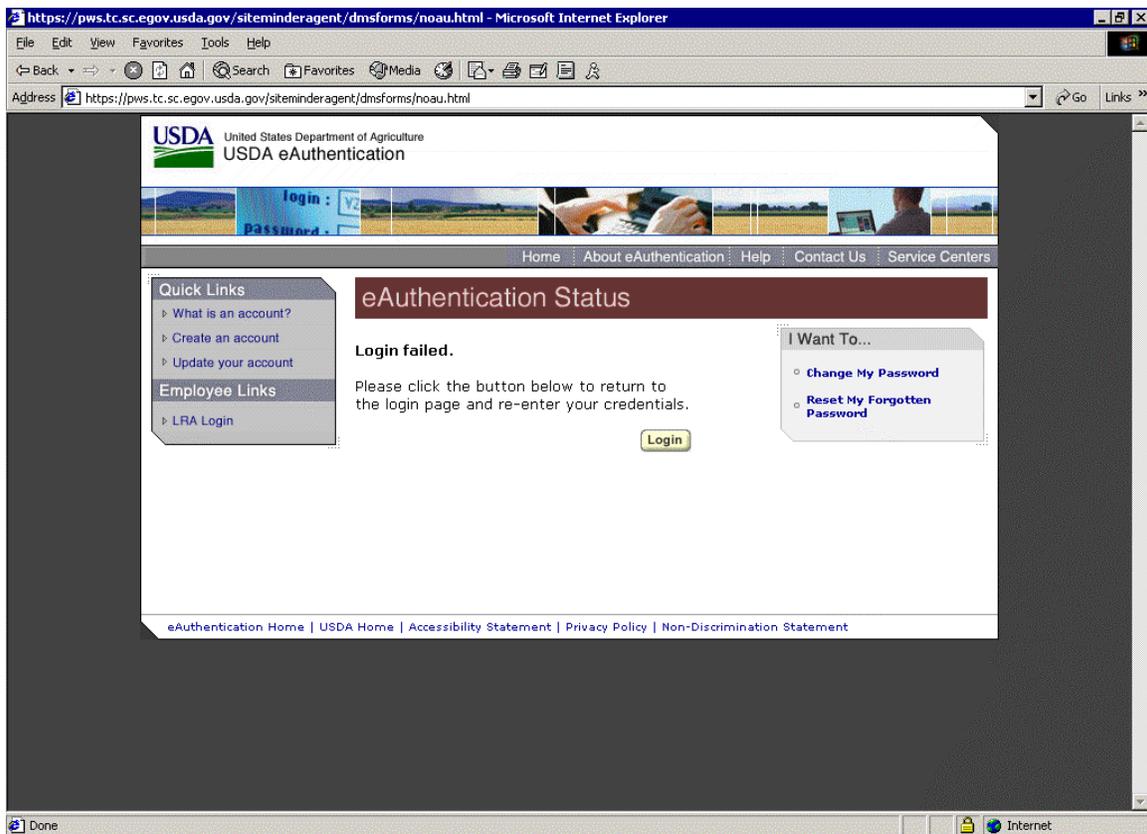
- If a user enters an invalid username and password, has insufficient credential level or application permissions required to access a page the **eAuthentication Status** page displays. For more information, please refer to Section 3.3.9: eAuthentication Status page.
- If a user clicks the **I want to Change My Password** link, the *Change Password* page displays. For more information, please refer to Section 3.5.6: Change My Password page and Section 3.6.1: Change Password page.

- If a user clicks the **I want to Reset My Forgotten Password** link, the *Forgotten Password* page displays. For more information, please refer to Section 3.6.2: Forgotten Password Recovery for Level 1 users and Section 3.6.3: Forgotten Password Recovery for Level 2 users.

3.3.9 eAuthentication Status page

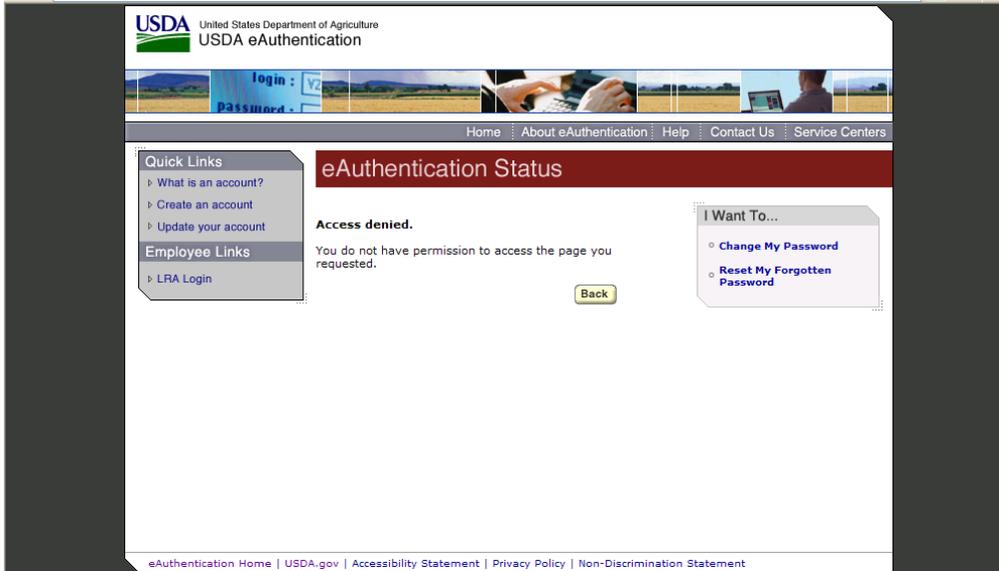
If a user enters credentials that are incorrect, attempts to log in and is not authorized to view a website due to lack of sufficient credential level or necessary application permissions the **eAuthentication Status** page displays.

If the user's credentials are incorrect the following version of the page displays:



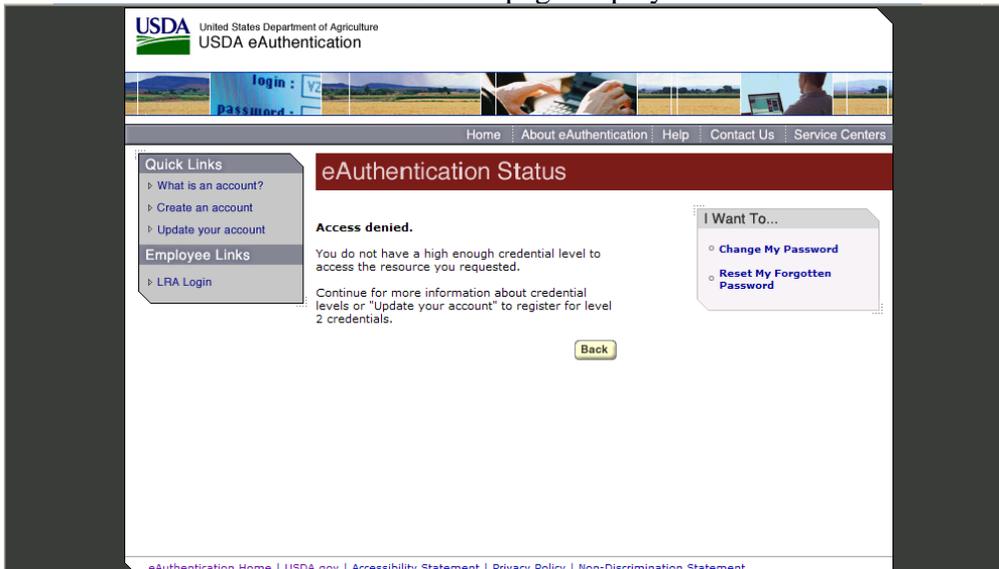
- If a user clicks the **Login** button, *the USDA Web Services Log-In* page displays. The user is able to re-enter their credentials. For more information, please refer to Section 3.3.8: USDA Web Services Log-In page.

If a user is denied access due to lack of sufficient credential level the following version of the **eAuthentication Status** page displays:



- If a user clicks the **Back** button, *the USDA Web Services Log-In* page displays. The user is able to re-enter their credentials. For more information, please refer to Section 3.3.8: USDA Web Services Log-In page.

If a user is denied access due to lack of necessary application permissions the following version of the **eAuthentication Status** page displays:



- If a user clicks the **Back** button, *the USDA Web Services Log-In* page displays. The user is able to re-enter their credentials. For more information, please refer to Section 3.3.8: USDA Web Services Log-In page.



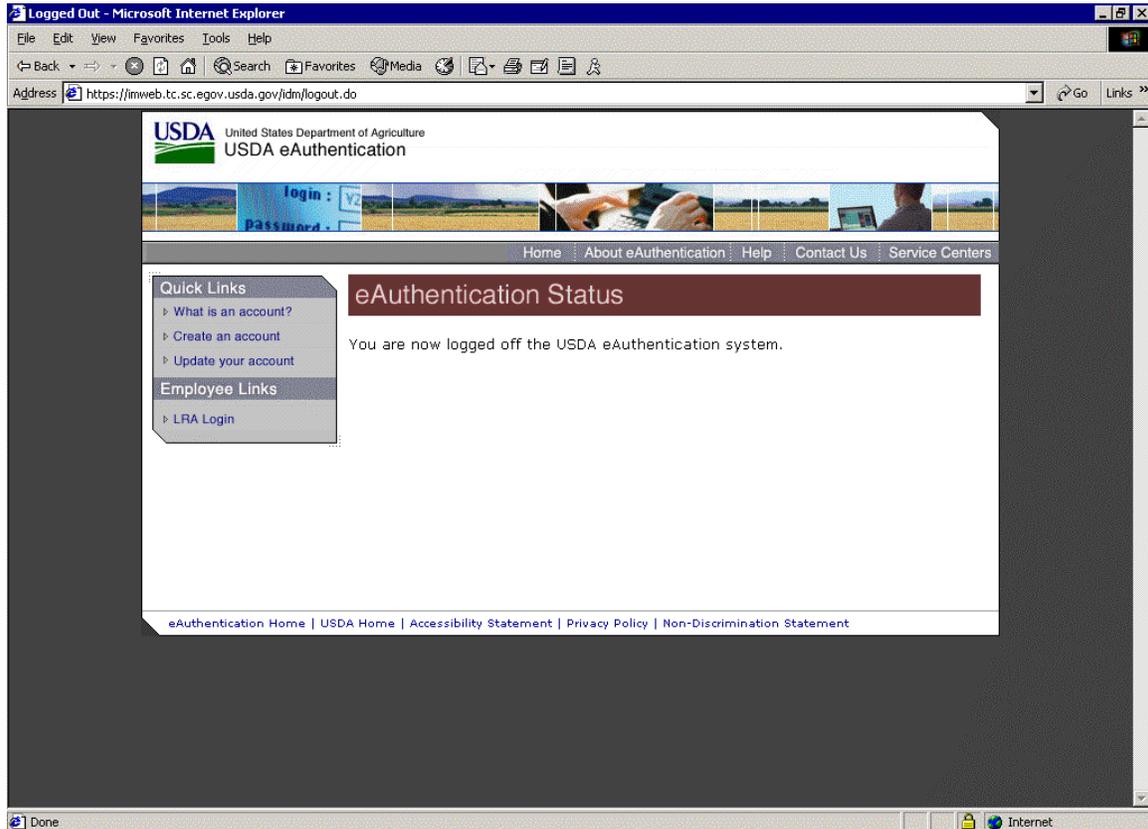
3.3.9.1 Custom Authorization Denied page

Application owners have the option of displaying customized authorization denied pages. These pages could contain specific messages to users of the application and information on why they do not have authorization. These pages could, for example, inform the user on how to obtain authorization and who to contact.

3.3.10 Logoff pages

3.3.10.1 Global Logoff page

When a user logs out of the USDA environment, the system displays the *Global Logoff* page. For more information, please, refer to Section 4.6.6: Build Logoff Page.



Once a user is logged out and see this *Default Logoff* page, they must re-enter their User ID and passwords to sign in again

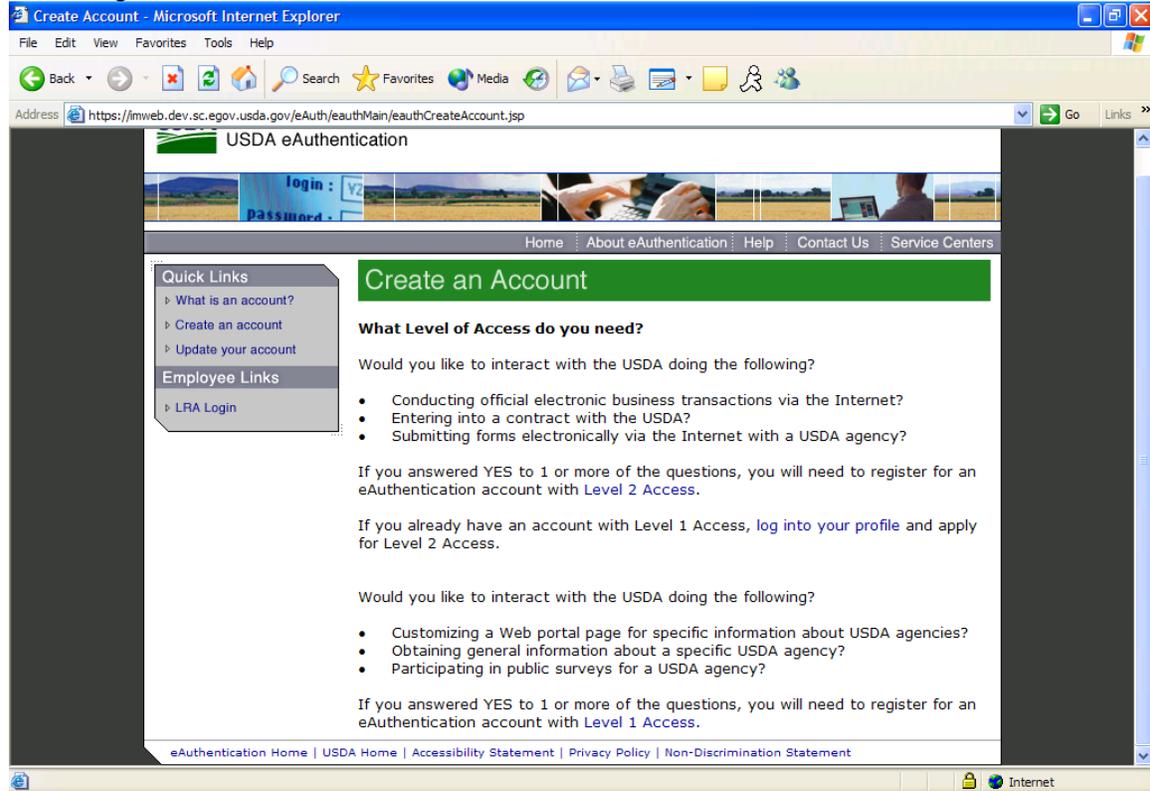
3.3.10.2 Local Logoff page

While the *Default Logoff* page is included and provided to all agencies, it is possible for agencies to create their own, *Custom Logoff* page. For more information, please refer to Section 5 Detailed Development Information.

3.4 Account Registration

3.4.1 Create Account page

The *Create Account* page displays when a user clicks the **Create an account** link on the left navigation bar.



This page helps users determine their registration needs and begin self-registration.

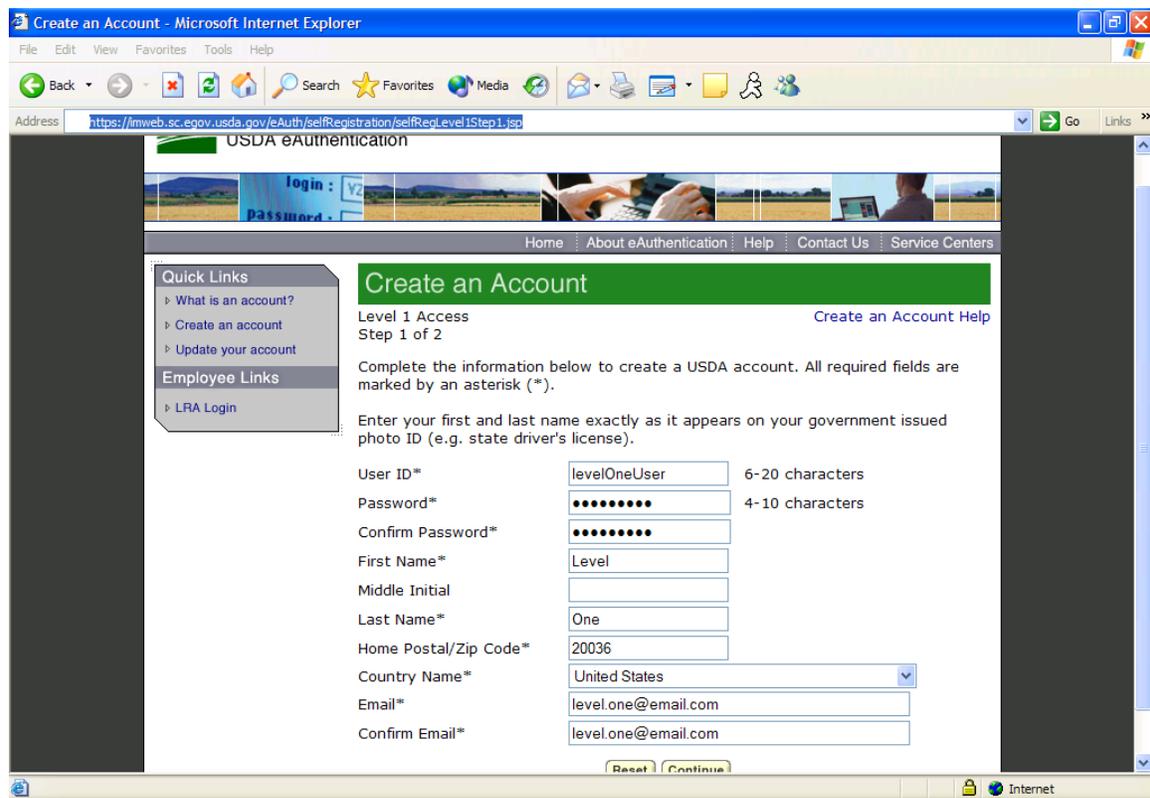
- If a user determines that they require Level 2 access, they can click on the **Level 2 Access** link and continue to register for an account. For more information, please refer to Section 3.4.5: Create an Account Level 2.
- If a user determines that they require Level 1 access, they can click on the **Level 1 Access** link and continue to register for an account. For more information, please refer to Section 3.4.2: Create an Account Level 1.
- If a user that already has level 1 access determines that they require Level 2 access, they can click the **Log into your Profile** link and apply for Level 2 access. For more information, please refer to Section 3.5.4: Apply for Level 2 Authentication page.

- If a user clicks the **What is an Account** link, the *What is an Account?* page displays. For more information, please refer to Section 3.3.6: What is an Account? page.

3.4.2 Create an Account Level 1

3.4.2.1 Create an Account Level 1 Access Step 1 page

If a user clicks the **Level 1 Access** link on the *Create Account* page the *Create an Account: Level 1 Access Step 1* page displays.



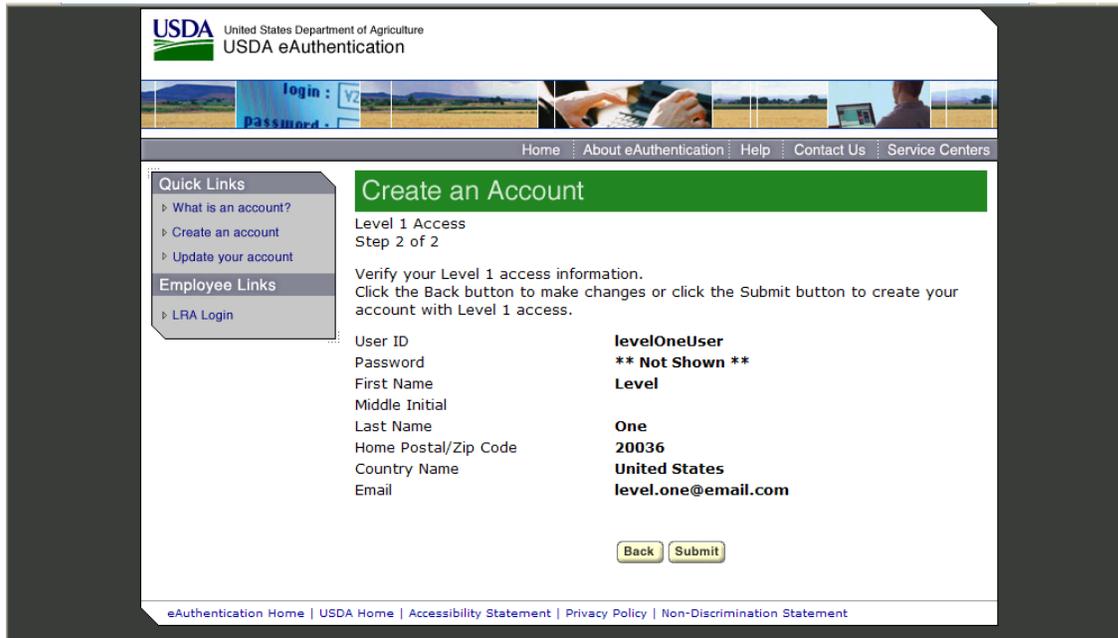
The screenshot shows a web browser window titled "Create an Account - Microsoft Internet Explorer". The address bar shows the URL: <https://imweb.sc.egov.usda.gov/eAuth/selfRegistration/selfRegLevel1Step1.jsp>. The page content includes a navigation menu with "Home", "About eAuthentication", "Help", "Contact Us", and "Service Centers". A "Quick Links" sidebar contains "What is an account?", "Create an account", "Update your account", and "Employee Links" with "LRA Login". The main heading is "Create an Account" with a sub-heading "Level 1 Access Step 1 of 2" and a "Create an Account Help" link. The instructions state: "Complete the information below to create a USDA account. All required fields are marked by an asterisk (*). Enter your first and last name exactly as it appears on your government issued photo ID (e.g. state driver's license)." The form fields are: User ID* (text box with "levelOneUser", 6-20 characters), Password* (password box with 10 dots, 4-10 characters), Confirm Password* (password box with 10 dots), First Name* (text box with "Level"), Middle Initial (text box), Last Name* (text box with "One"), Home Postal/Zip Code* (text box with "20036"), Country Name* (dropdown menu with "United States"), Email* (text box with "level.one@email.com"), and Confirm Email* (text box with "level.one@email.com"). At the bottom are "Reset" and "Continue" buttons.

This page contains a form that a user must complete to register for an account with Level 1 access. The asterisks denote required fields.

- If a user clicks the **Reset** button at any time, all fields in the form clear and the user is able to retype all information into the fields.
- If a user fills in all of the required fields and then clicks the **Continue** button, the *Create an Account: Level 1 Access Step 2* page displays.

3.4.2.2 Create an Account: Level 1 Access Step 2 page

If a user fills in all of the required fields on the *Create an Account Level 1 Access Step 1* page and then clicks the **Continue** button, the *Create an Account: Level 1 Access Step 2* page displays.

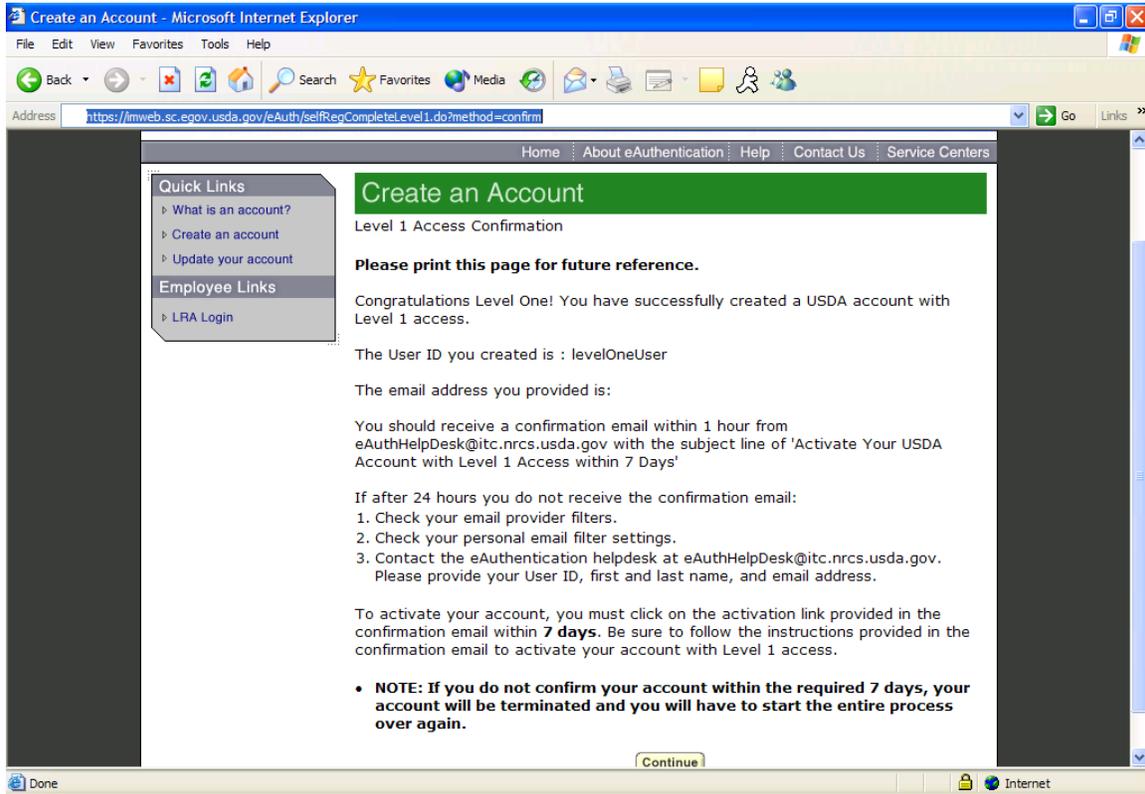


The *Create an Account: Level 1 Access* page displays a summary of the information entered. The user must confirm that they entered the correct information.

- If a user clicks the **Back** button, the *Create an Account: Level 1 Access Step 1* page displays. The user is able to change the data previously entered.
- If a user confirms that the information shown is correct, they can click on **Submit** button. If a user clicks on the **Submit** button, the *Create an Account: Level 1 Access Confirmation* page displays.

3.4.2.3 Create an Account: Level 1 Access Confirmation page

If a user clicks on the **Submit** button on the *Create an Account: Level 1 Access Step 2* page, the *Create an Account: Level 1 Access Confirmation* page displays.

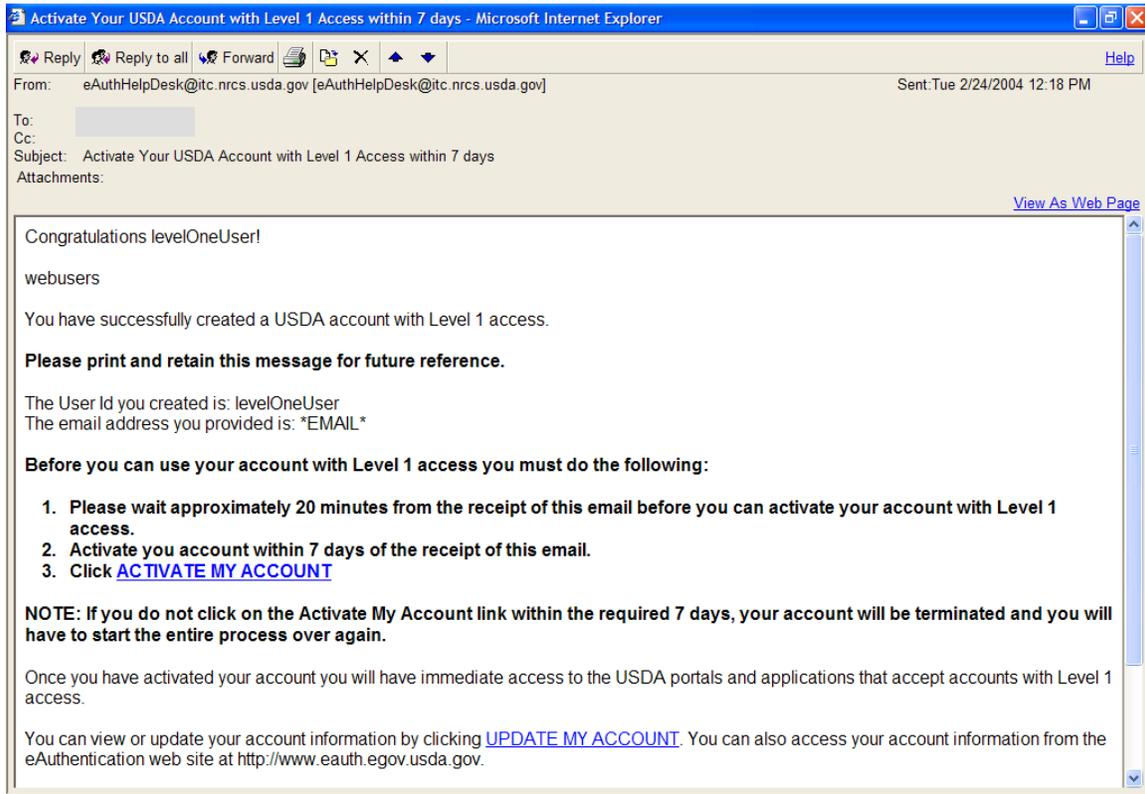


The *Create an Account: Level 1 Access Confirmation* page displays confirmation that an account has been created. It also displays instructions required to activate a level 1 account.

- If a user clicks the **Continue** button, the *eAuthentication Home* page displays.

3.4.3 Account Creation Confirmation Email

The *Account Creation Confirmation Email* is sent to the user email address after they register online.

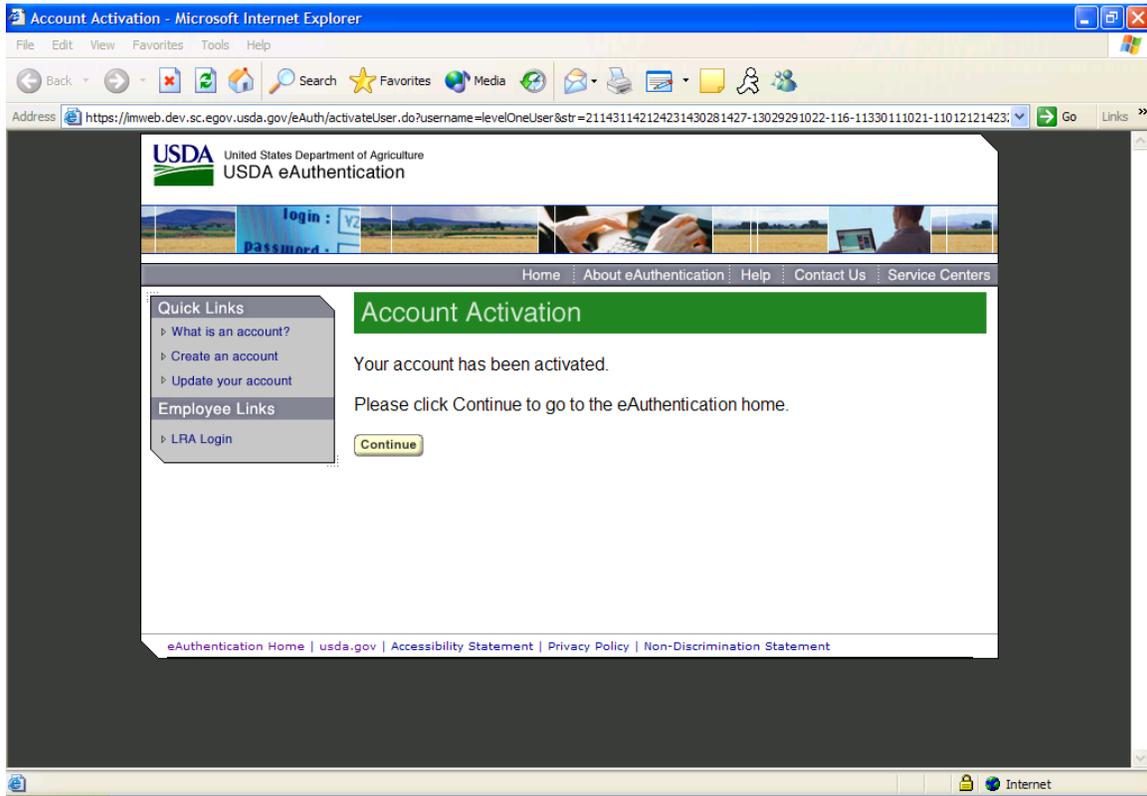


The *Account Creation Confirmation Email* contains instructions that explain how to activate an account, links for activating and updating an account, and instructions on how to contact the Help Desk.

- If a user clicks the **Activate My Account** link, the *Account Activation* page displays.
- If a user clicks the **Update My Account** link, the *USDA Web Services Log-In* page displays. For more information, please refer to Section 3.5: Account Management.

3.4.4 Account Activation page

If a user clicks the **Activate My Account** link in their *Account Creation Confirmation Email* the *Account Activation* page displays

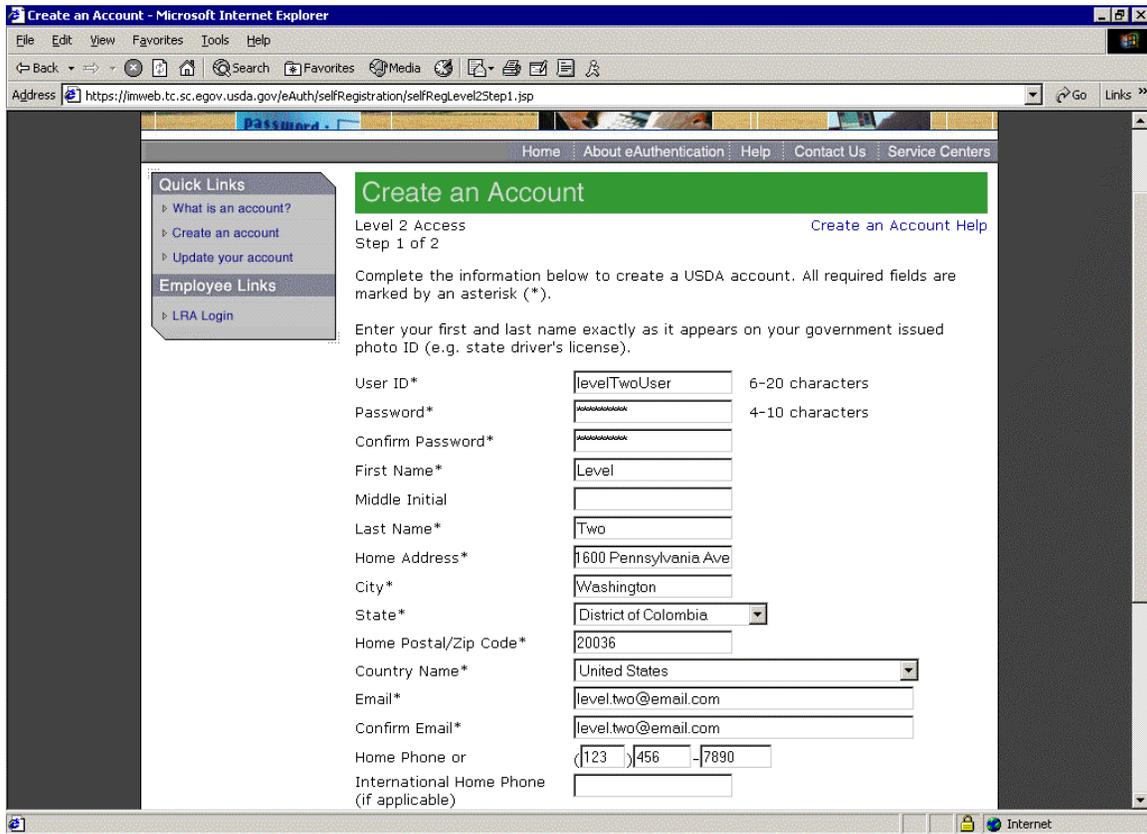


- If a user clicks on the **Continue** button, the *eAuthentication Home* page displays.

3.4.5 Create an Account Level 2

3.4.5.1 Create an Account Level 2 Step 1 page

If a user clicks the **Level 2 Access** link on the *Create Account* page the *Create an Account: Level 2 Access Step 1* page displays.

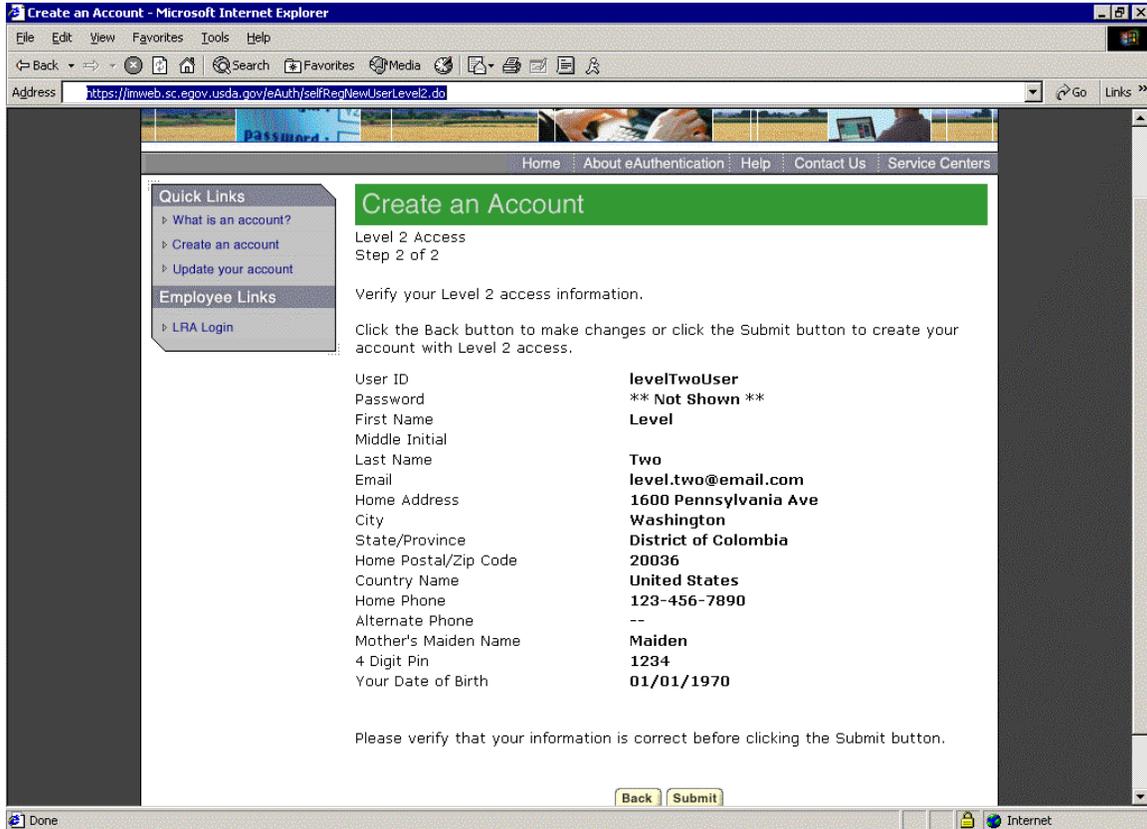


This page contains a form that a user must complete to register for an account with Level 2 access. The asterisk denotes required fields. Note that more information is needed for Level 2 registration than was necessary for Level 1.

- If a user clicks the **Reset** button at any time, all fields in the form clear and the user is able to retype all information into the fields.
- If a user confirms that the information shown is correct, they can click on **Submit** button. If a user clicks on the **Submit** button, the *Create an Account: Level 2 Access Step 2* page displays.

3.4.5.2 Create an Account: Level 2 Access Step 2 page

If a user clicks on the **Submit** button on the *Create an Account: Level 2 Access Step 1* page, the *Create an Account: Level 2 Access Step 2* page displays.

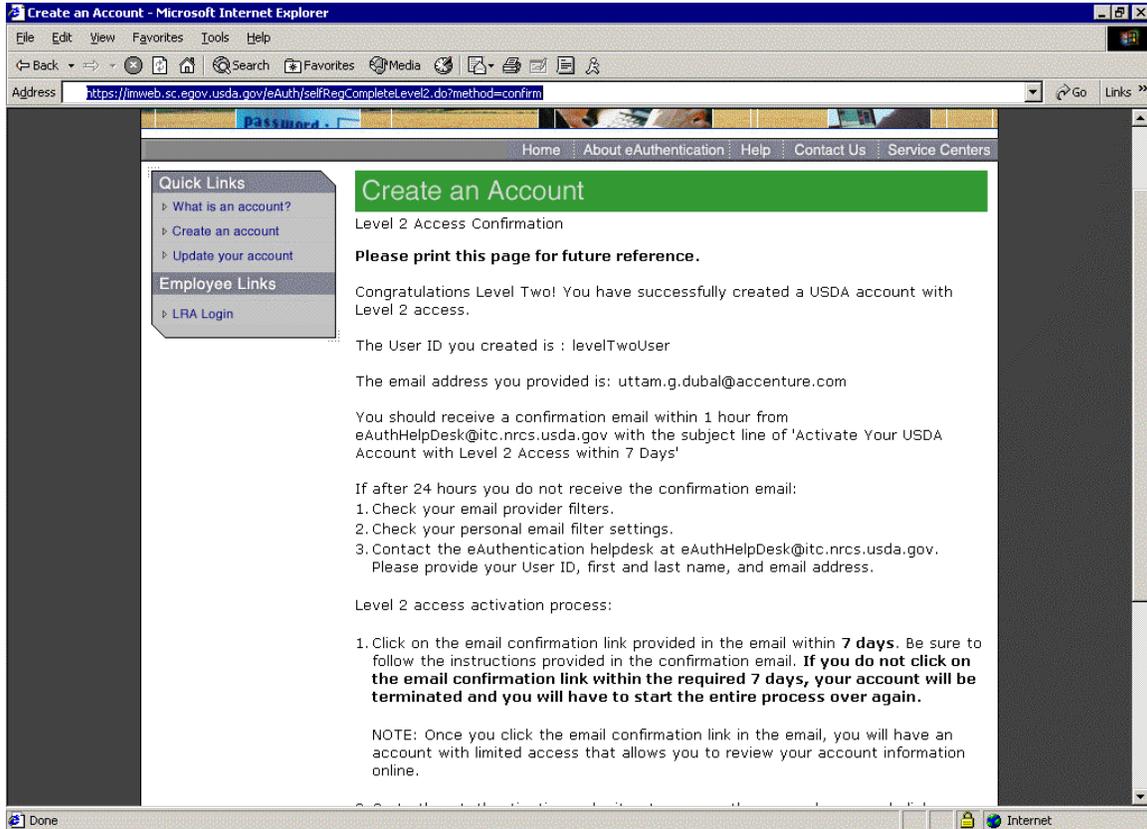


The *Create an Account: Level 2 Access Step 2* page displays a summary of the information entered. The user must confirm that they entered the correct information.

- If a user clicks the **Back** button, the *Create an Account: Level 2 Access Step 1* page displays. The user is able to change the data previously entered.
- If a user confirms that the information shown is correct, they can click on **Submit** button. If a user clicks on the **Submit** button, the *Create an Account: Level 2 Access Confirmation* page displays.

3.4.5.3 Create an Account: Level 1 Access Confirmation

If a user clicks on the **Submit** button on the *Create an Account: Level 2 Access Step 2* page, the *Create an Account: Level 2 Access Confirmation* page displays.

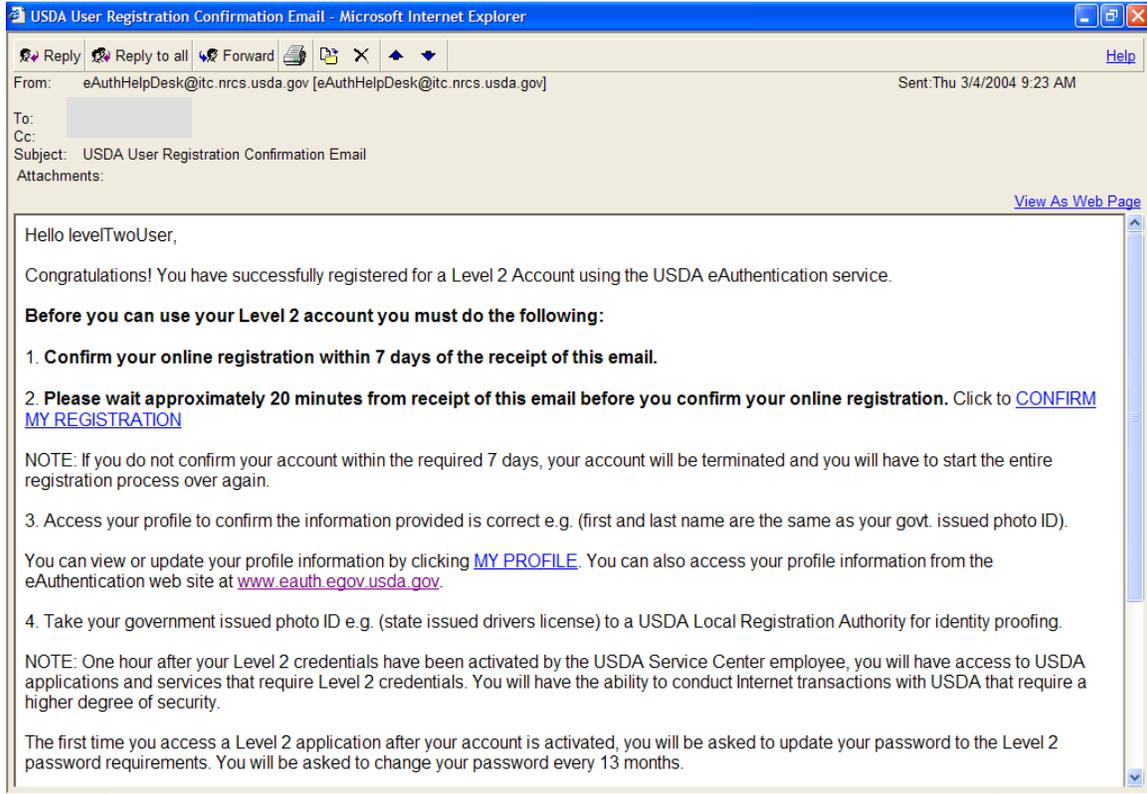


The *Create an Account: Level 2 Access Confirmation* page displays confirmation that an account has been created. It also displays instructions required to activate a level 2 account.

- If a user clicks the **Continue** button, the *eAuthentication Home* page displays.

3.4.6 Account Creation Confirmation Email

The *Account Creation Confirmation Email* is sent to the user email address after they register online.



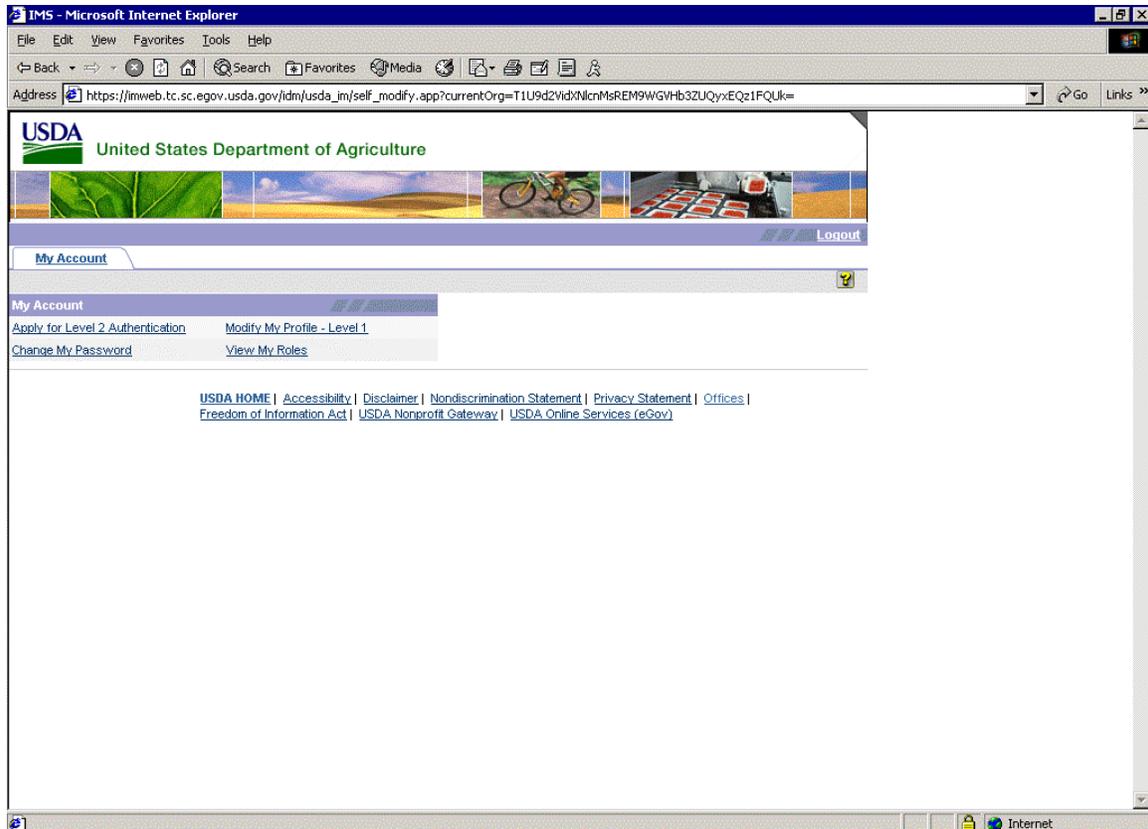
The *Account Creation Confirmation Email* contains instructions that explain how to activate an account, links for activating and updating an account, and instructions on how to contact the Help Desk.

- If a user clicks the **Activate My Account** link, the *Account Activation* page displays. It is important to note that users are first given Level 1 Assurance when they complete level 2 registration. It is not until they go to a service center show a proper type of identification that they are given Level 2 assurance. For more information, please refer to Section 4.7: Registration Certification.
- If a user clicks the **Update My Account** link, the *USDA Web Services Log-In* page displays. For more information, please refer to Section 3.5: Account Management.

3.5 Account Management

3.5.1 IMS page

If a user clicks on the **Update Your Account** link the left navigation bar the *The USDA Web Services Log-In Warning!* page displays. If a users logs in, the *Identity Management Services (IMS)* page displays.



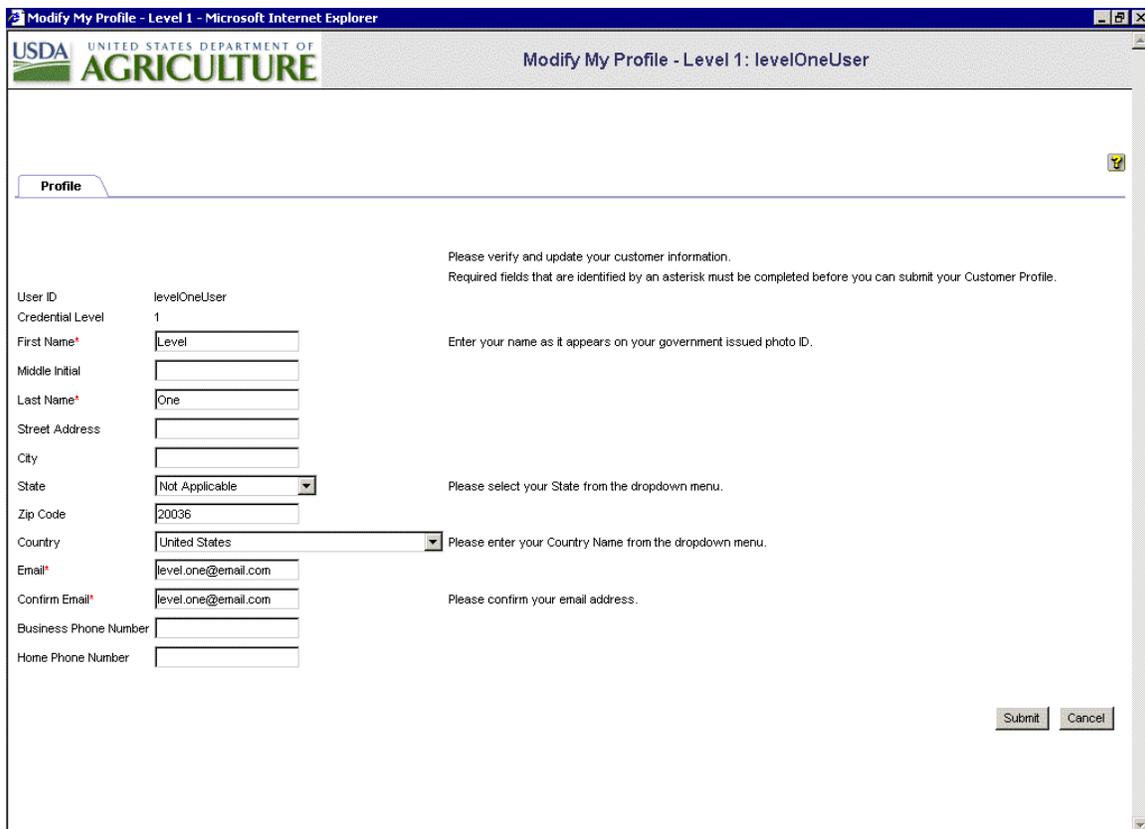
The *IMS* page allows the user to log in to their account and take a number of actions pertinent to their account type and user needs. If a user clicks on the **My Account** link, the *My Account* tab displays the user’s tasks which can include:

- **Modify My Profile** – This function allows the user to change their eAuthentication user account attributes. For more information, please refer to Section 3.5.2: Modify my Profile – Level 1 page.
- **Apply for Level 2 Authentication** – This function allows Level 1 users to enter the information needed to register for Level 2 assurance. This is only an option for users logged in with Level 1 assurance. For more information, please refer to Section 3.5.3: Modify my Profile – Level 2 page.

- **Change My Password** – This function allows users to change their password to a new password specified by the user. For more information, please refer to Section 3.5.6: Change My Password page.
- **View My roles** – This function allows users to view the roles that they have been assigned. For more information, please refer to Section 3.5.5: View my Roles page.

3.5.2 Modify my Profile – Level 1 page

If a user clicks the **Modify My Profile – Level 1** link on the *IMS* page, the *Modify My Profile – Level 1* page opens.



Profile

Please verify and update your customer information.
Required fields that are identified by an asterisk must be completed before you can submit your Customer Profile.

User ID: levelOneUser
 Credential Level: 1

First Name* Enter your name as it appears on your government issued photo ID.
 Middle Initial
 Last Name*
 Street Address
 City
 State: Please select your State from the dropdown menu.
 Zip Code:
 Country: Please enter your Country Name from the dropdown menu.
 Email*
 Confirm Email* Please confirm your email address.
 Business Phone Number
 Home Phone Number

The *Modify My Profile – Level 1* page allows users to change their eAuthentication user information. A Level 1 user may overwrite/modify any of the fields except for the **User ID** field.

- If a user clicks the **Submit** button the changes will be made to the user account and the *Acknowledgement Message* page displays.
- If a user clicks the **Cancel** button no changes are made and the window closes.

3.5.3 Modify my Profile – Level 2 page

If a user clicks the **Modify My Profile – Level 2** link on the *USDA Identity Management Services (IMS)* page, the *Modify My Profile – Level 2* page opens. The *Modify My Profile – Level 2* page allows users to change their eAuthentication user attributes. If a Level 2 user chooses to modify their profile, the options provided are slightly different than those for a level 1 user.



Profile

Please verify and update your customer information.
Required fields that are identified by an asterisk must be completed before you can submit your Customer Profile.

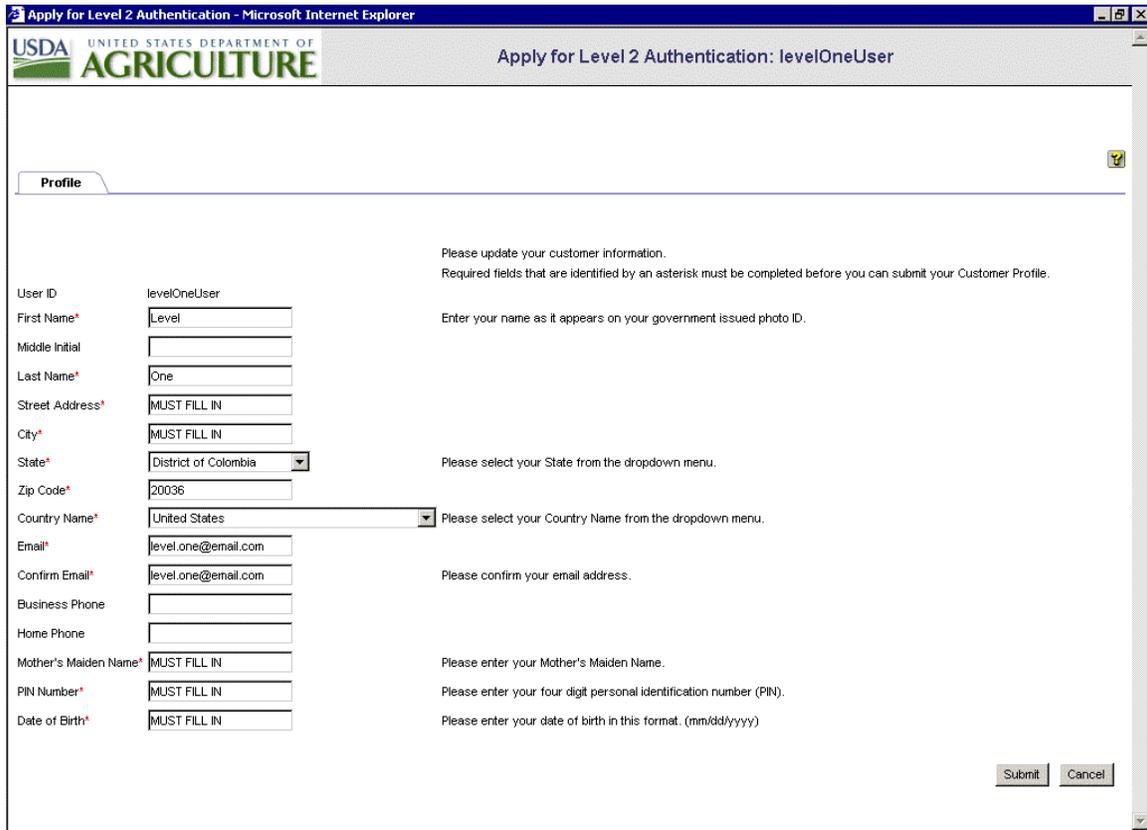
User ID	levelTwoUser	
Credential Level	2	
First Name	Level	
Middle Initial		
Last Name	Two	
Street Address*	<input type="text" value="1600 Pennsylvania Ave"/>	
City*	<input type="text" value="Washington"/>	
State*	<input type="text" value="District of Columbia"/>	Please select your State from the dropdown menu.
Zip Code*	<input type="text" value="20036"/>	
Country*	<input type="text" value="United States"/>	Please enter your Country Name from the dropdown menu.
Email*	<input type="text" value="level.two@email.com"/>	
Confirm Email*	<input type="text" value="level.two@email.com"/>	Please confirm your email address.
Business Phone Number	<input type="text" value="--"/>	
Home Phone Number	<input type="text" value="123-456-7890"/>	

Because Level 2 users have already been identity proofed the **User ID** field, **First Name** field, and **Last Name** field are read-only. Any of the other fields can be overwritten with new information. For more information, please refer to Section 4.7: Registration Certification.

- If a user clicks the **Submit** button the changes will be made to the user account and the *Acknowledgement Message* page displays.
- If a user clicks the **Cancel** button at any time the window will close.
- If a user clicks the **Close Window** button at any time the window will close and the user will again see the *USDA Identity Management Services (IMS)* page.

3.5.4 Apply for Level 2 Authentication page

If a user clicks the **Apply for Level 2 Authentication** link on the *USDA Identity Management Services (IMS)* page, the *Apply for Level 2 Authentication* page opens.



Profile

Please update your customer information.
Required fields that are identified by an asterisk must be completed before you can submit your Customer Profile.

User ID: levelOneUser

First Name* Enter your name as it appears on your government issued photo ID.

Middle Initial

Last Name*

Street Address*

City*

State* Please select your State from the dropdown menu.

Zip Code*

Country Name* Please select your Country Name from the dropdown menu.

Email*

Confirm Email* Please confirm your email address.

Business Phone

Home Phone

Mother's Maiden Name* Please enter your Mother's Maiden Name.

PIN Number* Please enter your four digit personal identification number (PIN).

Date of Birth* Please enter your date of birth in this format. (mm/dd/yyyy)

The **Apply for Level 2 Authentication** page is only available to users logged in with Level 1 assurance. Level 1 users enter additional, required information about themselves as part of the process of upgrading from Level 1 to Level 2. Users then go to Service Centers where they are identity proofed and given Level 2 Assurance.

Users wanting to apply for Level 2 Authentication must fill out all of the additional fields marked by a red asterisk.

- If a user clicks the **Submit** button, the *Acknowledgement Message* page displays.
- If a user clicks the **Cancel** button at any time, the window closes.

3.5.5 View my Roles page

When a user clicks on the **View My Roles** link on the *Identity Management Services (IMS)* page, the *View My Roles - Profile* page opens. The *View My Roles - Profile* page allows all users to see a summary of the roles to which they (1) have been assigned and (2) have the ability to assign to other users.

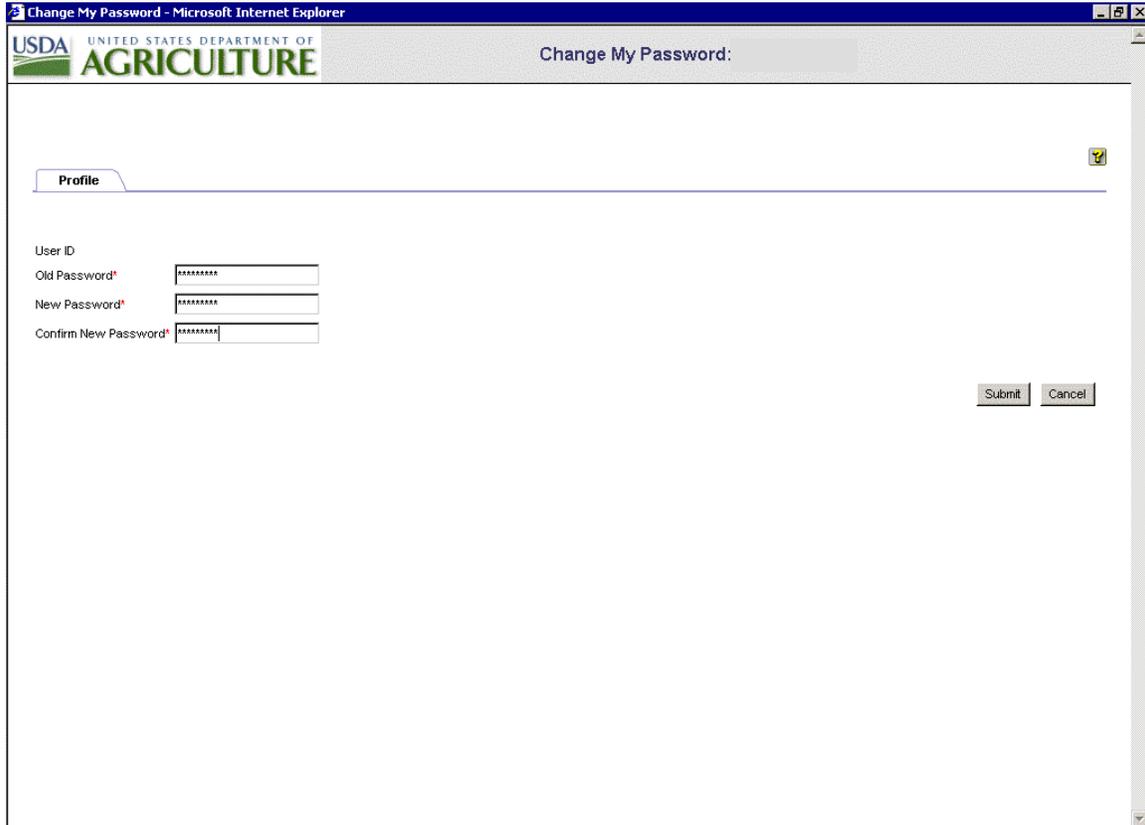


Users wanting to view their roles are first shown their basic user Profile under the **Profile** tab. In the basic user profile are stated the user's username, First Name and Last Name.

- The **Next** button contains no pertinent functionality.
- If a user clicks the **Close** button at any time, the window closes.
- If a user clicks the **Local Admin Roles** tab the user's system administrator roles display.
- If a user clicks the **Access Roles** tab the user's access roles related to application permissions display.

3.5.6 Change My Password page

If a user clicks the **Change my Password** link on the *USDA Identity Management Services (IMS)* page, the *Change My Password* page opens. For more information, please refer to Section 3.5: Account Management.



The screenshot shows a web browser window titled "Change My Password - Microsoft Internet Explorer". The page header includes the USDA logo and the text "UNITED STATES DEPARTMENT OF AGRICULTURE". The main content area is titled "Change My Password:" and features a "Profile" tab. Below the tab, there is a form with the following fields: "User ID", "Old Password*", "New Password*", and "Confirm New Password*", each with a corresponding input field. At the bottom right of the form, there are "Submit" and "Cancel" buttons.

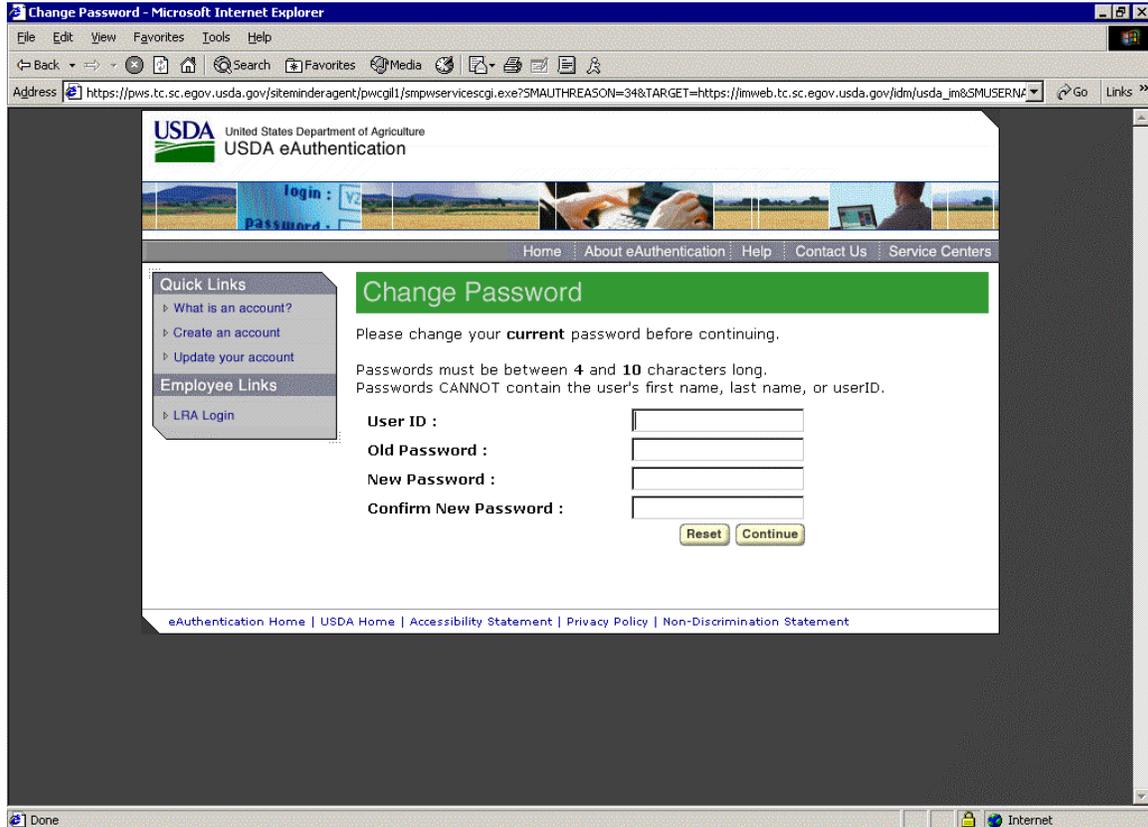
To change their password, the user must first enter their current password in the **Old Password** field. The user must then enter their new password in both the **New Password** and **Confirm New Password** fields.

- If a user clicks the **Submit** button, the system attempts to change their password. If the correct current password was entered and if both the **New Password** and **Confirm New Password** fields are identical the password is changed and the *Acknowledgement Message* page displays.
- If a user clicks the **Cancel** button at any time, the window will close.

3.6 Password Maintenance

3.6.1 Change Password page

If a user clicks the *Change My Password* link on the *USDA Web Services Log-In* page, and then logs in, the *Change Password* page displays.



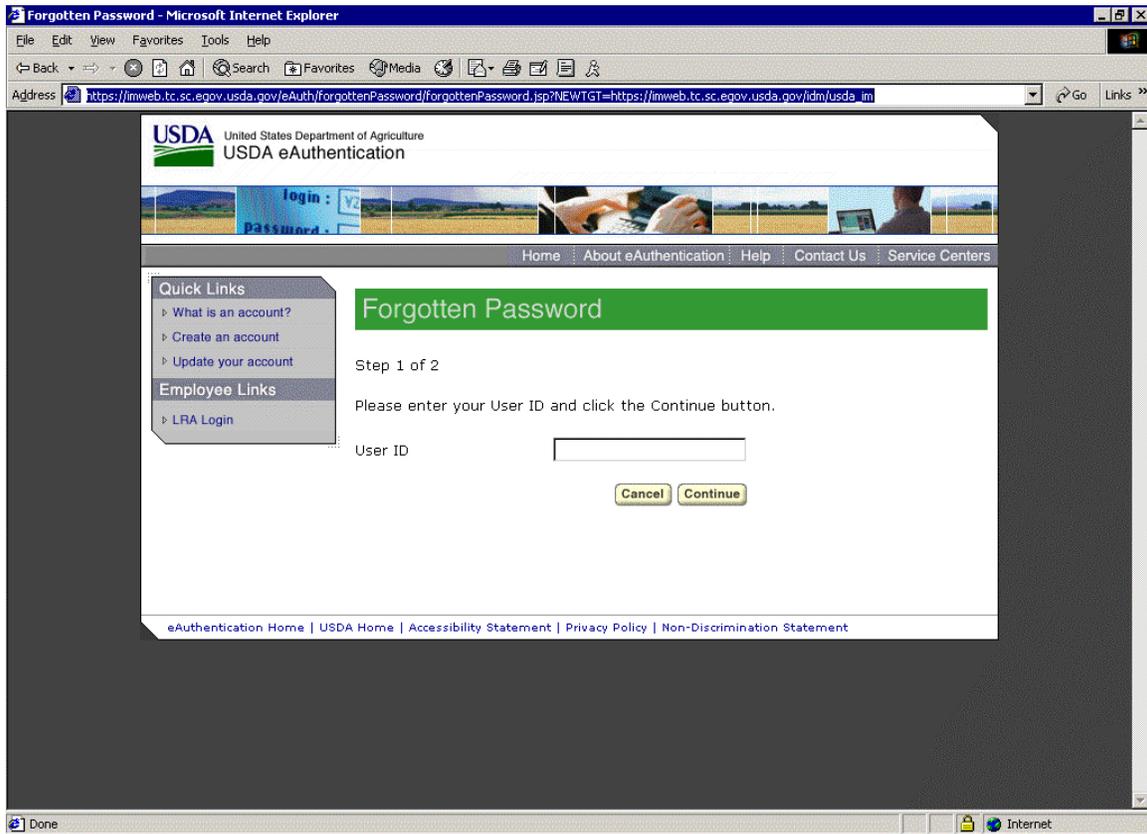
To change their password, the user must first enter their user name in the **User ID** field and their current password in the **Old Password** field. The user must then enter their new password in both the **New Password** and **Confirm New Password** fields. It is important to note that Level 2 users are required to use strong passwords.

- If a user clicks the **Reset** button at any time, all fields in the form clear and the user is able to retype all information into the fields.
- If a user clicks the **Continue** button after filling in all the fields, the *Change Password Confirmation* page displays indicating that a new password has been set.

3.6.2 Forgotten Password Recovery for Level 1 users

3.6.2.1 Forgotten Password Level 1 Log-In page

If a user clicks the **Reset My Forgotten Password** link on the *USDA Web Services Log-In* page the *Forgotten Password Log-In Level 1* page displays.

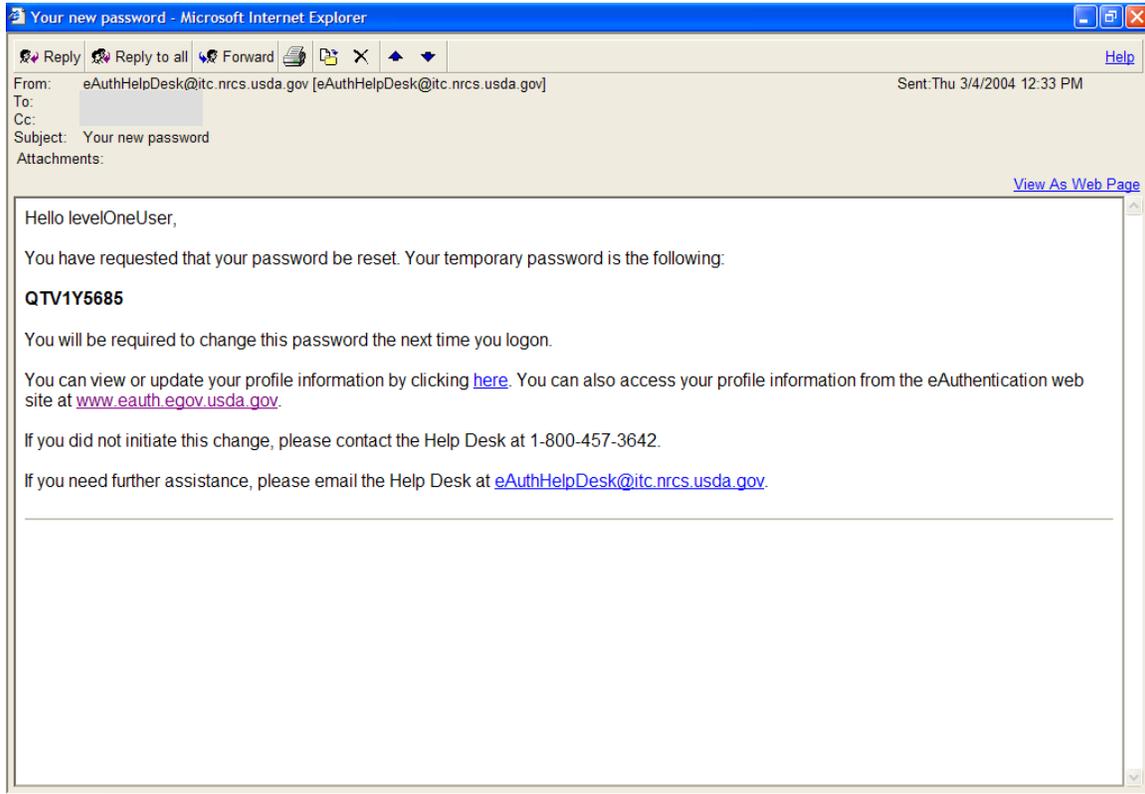


By entering their username in the **User ID** field, users can begin the request to set their password to a random, system-generated password. The user can use this temporary password, sent to their email address, to log in and change their password to a user specified password.

- If a user clicks the **Continue** button, the user is asked if they are sure that they would like to reset their password. If the user confirms the change the password is sent to their email address.
- If a user clicks the **Cancel** button, the *USDA Web Services Log-In Warning* page displays.

3.6.2.2 Temporary Password Email

The *Temporary Password Email* contains the newly generated, temporary user password. This is the password a user must enter after resetting the password.

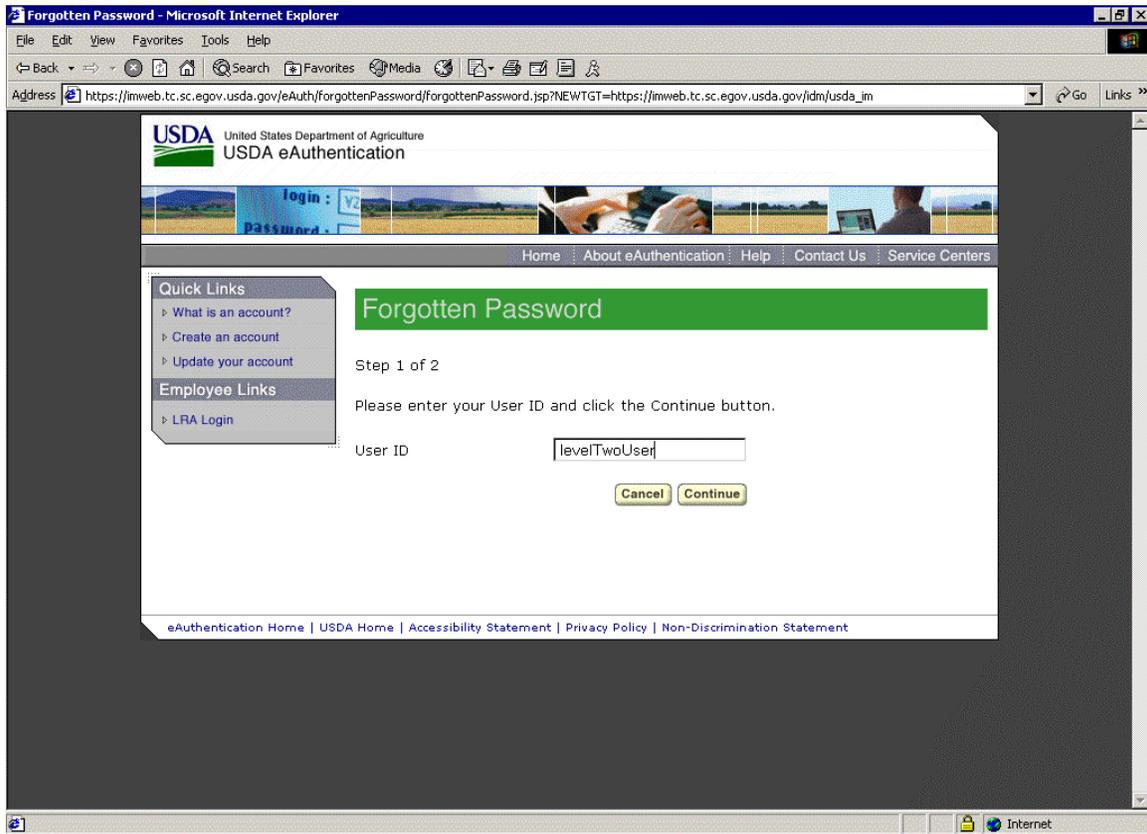


- If a user clicks the **here** link in the *Temporary Password Email*, the user is prompted to log-in with their new password. As soon as the user logs-in, they are forwarded to the *USDA Web Services Change Your Password* page in order to change their password.

3.6.3 Forgotten Password Recovery for Level 2 users

3.6.3.1 Forgotten Password Log-In Level 2 Step 1 page

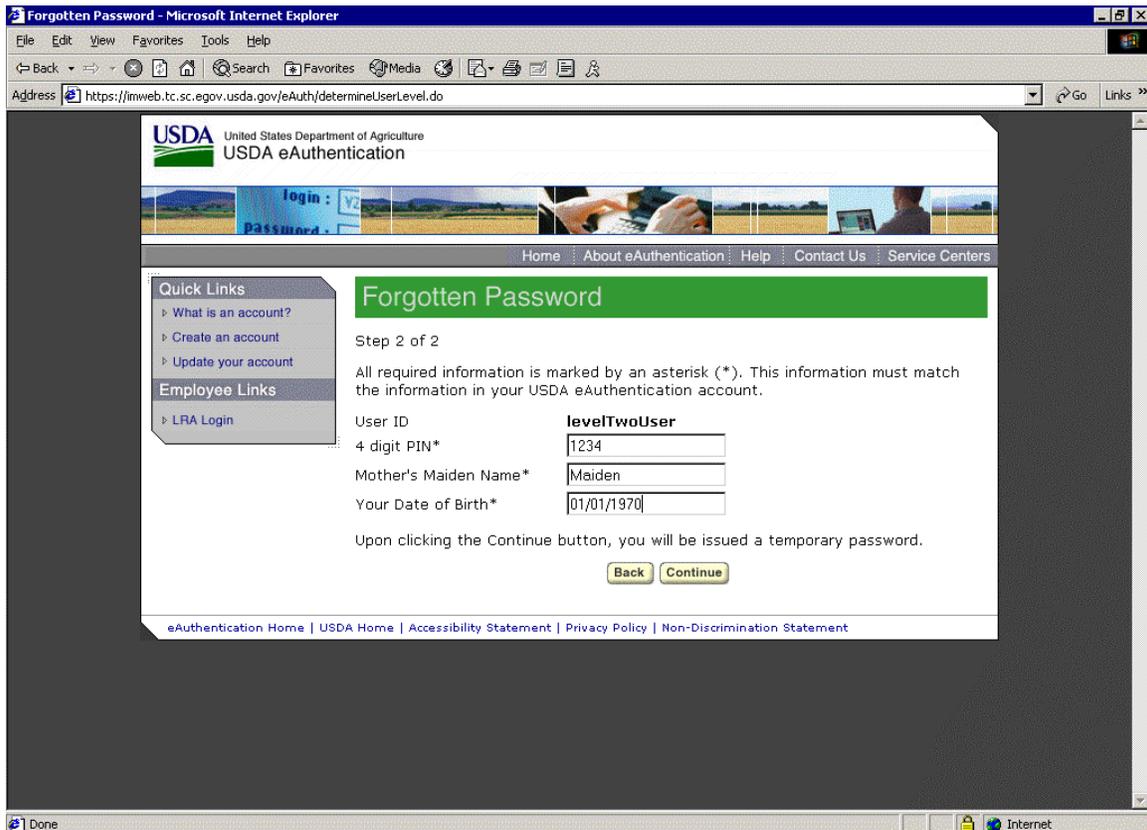
If a user clicks the **Reset My Forgotten Password** link on the *USDA Web Services Log-In* page the *Forgotten Password Log-In Level 2 Step 1* page displays.



- By entering their username in the **User ID** field, users are able to reset their password to a random, system-generated password. If a Level 2 user clicks the **Continue** button, they are asked for their username on the *Forgotten Password Log-In Level 2 Step 2* page. On that page the user is asked to enter their specific attributes (maiden name, PIN, and birth date). If the user attributes match with what is in the system, the new, temporary password is displayed to the user.
- If a user clicks the **Cancel** button, the *USDA Web Services Log-In Warning* page displays.

3.6.3.2 Forgotten Password Log-In Level 2 Step 2

If a user enters their User ID on the *Forgotten Password Log-In Level 2 Step 1* page and clicks the **Continue** button, the *Forgotten Password Log-In Level 2 Step 2* page displays.



The *Forgotten Password Log-In Level 2 Step 2* page asks the Level 2 user to confirm that they want to reset their forgotten password by asking for their specific user attributes (maiden name, PIN, and birth date).

- If a user clicks the **Back** button at any time, they are redirected to the previous page that was viewed on their browser.
- If a user clicks the **Continue** button, the user is issued a temporary password.



3.7 Administrative Accounts

3.7.1 Local Registration Authority

Local Registration Authorities (LRAs) have the ability to update assurance levels of users from level 1 to level 2 after users supply them proof of identity at one of many service centers.

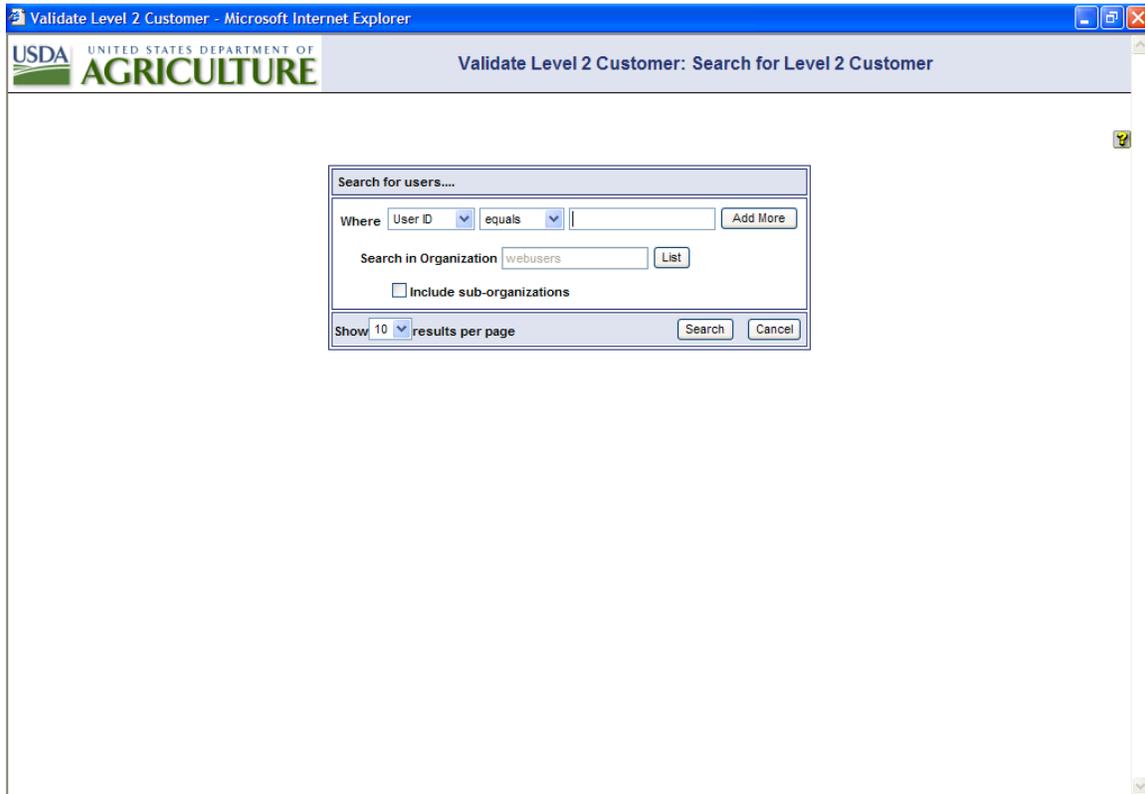
To perform LRA tasks, authorized users must log in with their LRA username when logging in at the *USDA Web Services Log-In* page. LRA Administrators are able to assign users level 2 credentials.

To use LRA tasks users should log in the same as normal users. If an LRA clicks the **My Tasks** tab on the *IMS* page, the different organizations for which they may assign Assurance Levels will display. In particular, the organization webusers should appear on the left side of their screen. If the user clicks the **webusers** link, the tasks display.

To change the assurance level of another user from Level 1 to Level 2, the LRA should click the **Validate Level 2 Customer** link on the *IMS* page.

3.7.2 Validate Level 2 Customer: Search for Level 2 Customer

If an LRA clicks the **Validate Level 2 Customer** link on the *IMS* page, the *Validate Level 2 Customer: Search for Level 2 Customer* page opens.

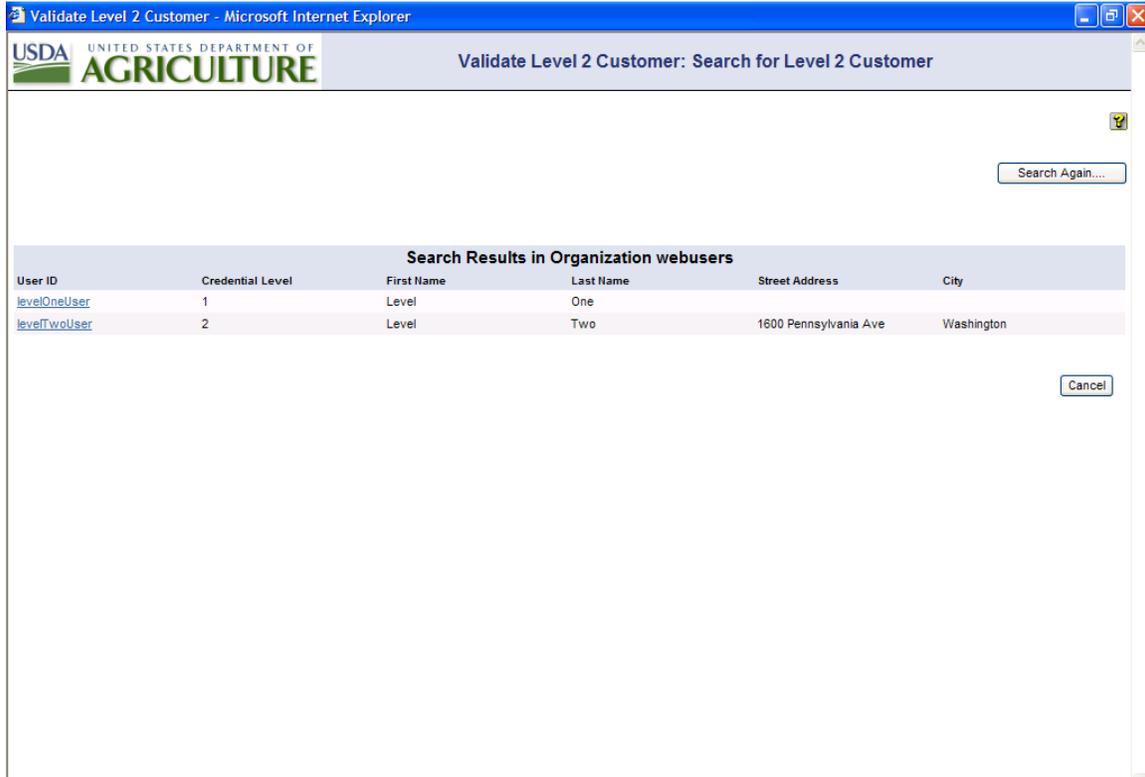


The *Validate Level 2 Customer: Search for Level 2 Customer* page allows an LRA Administrator to search for a user. The LRA Administrator can select a search attribute (Username, Last Name, First Name, or State) from the **Where** drop-down menu. The LRA Administrator can select a comparison attribute (**equals**, **starts with**, **ends with**, or **contains**) from the middle drop-down menu. The LRA Administrator enter the text to search for in the text box to the right of the other two fields.

- If the LRA Administrator clicks the **Search** button the *Search Results in Organization* page displays.

3.7.3 Search Results in Organization page

If an LRA clicks the **Search** button on the *Validate Level 2 Customer: Search for Level 2 Customer* page, the *Search Results in Organization* page displays.

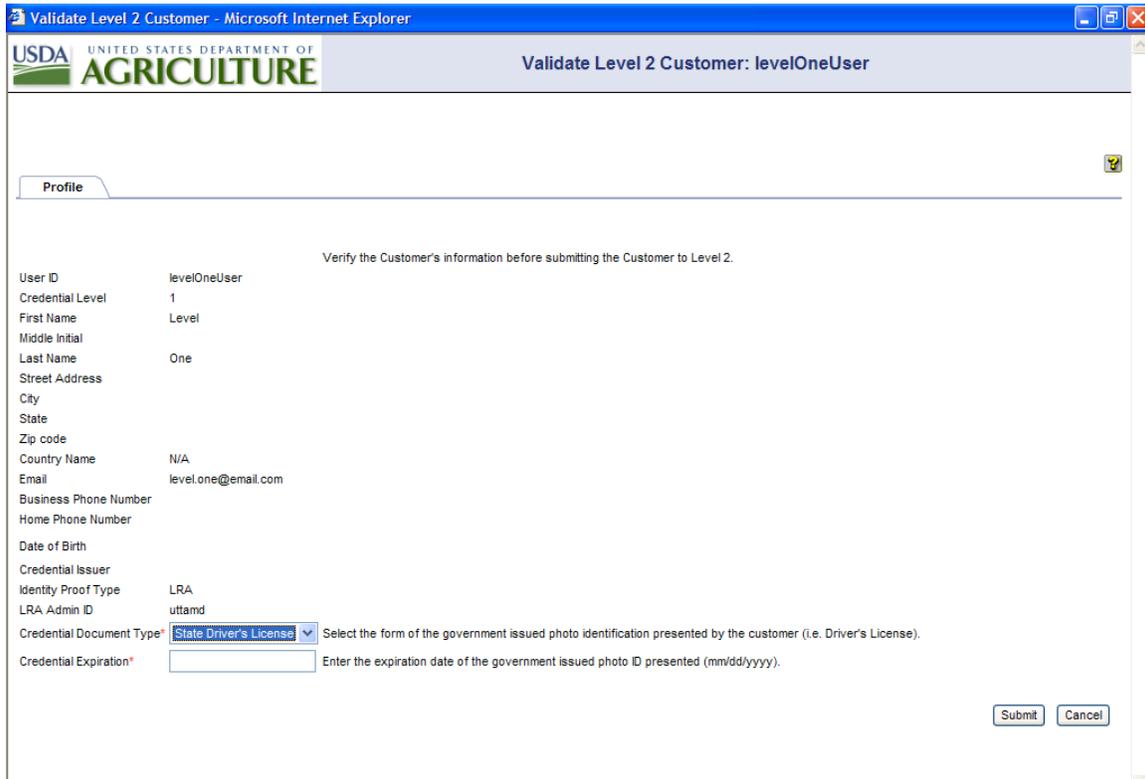


The *Search Results in Organization* page shows all users in the organization that match the specified search criteria entered on the *Validate Level 2 Customer: Search for Level 2 Customer* page. An LRA Administrator is able to select which of the users they want to validate as a Level 2 user.

- If a user clicks on one of the usernames shown in the list, the *Validate Level 2 Customer* page displays with the corresponding user's information.

3.7.4 Validate Level 2 Customer page

If a user clicks one of the usernames shown on the *Search Results in Organization* page, the *Validate Level 2 Customer* page displays.



Validate Level 2 Customer - Microsoft Internet Explorer

USDA UNITED STATES DEPARTMENT OF AGRICULTURE

Validate Level 2 Customer: levelOneUser

Profile

Verify the Customer's information before submitting the Customer to Level 2.

User ID	levelOneUser
Credential Level	1
First Name	Level
Middle Initial	
Last Name	One
Street Address	
City	
State	
Zip code	
Country Name	N/A
Email	level.one@email.com
Business Phone Number	
Home Phone Number	
Date of Birth	
Credential Issuer	
Identity Proof Type	LRA
LRA Admin ID	uttamd
Credential Document Type*	State Driver's License Select the form of the government issued photo identification presented by the customer (i.e. Driver's License).
Credential Expiration*	Enter the expiration date of the government issued photo ID presented (mm/dd/yyyy).

Submit Cancel

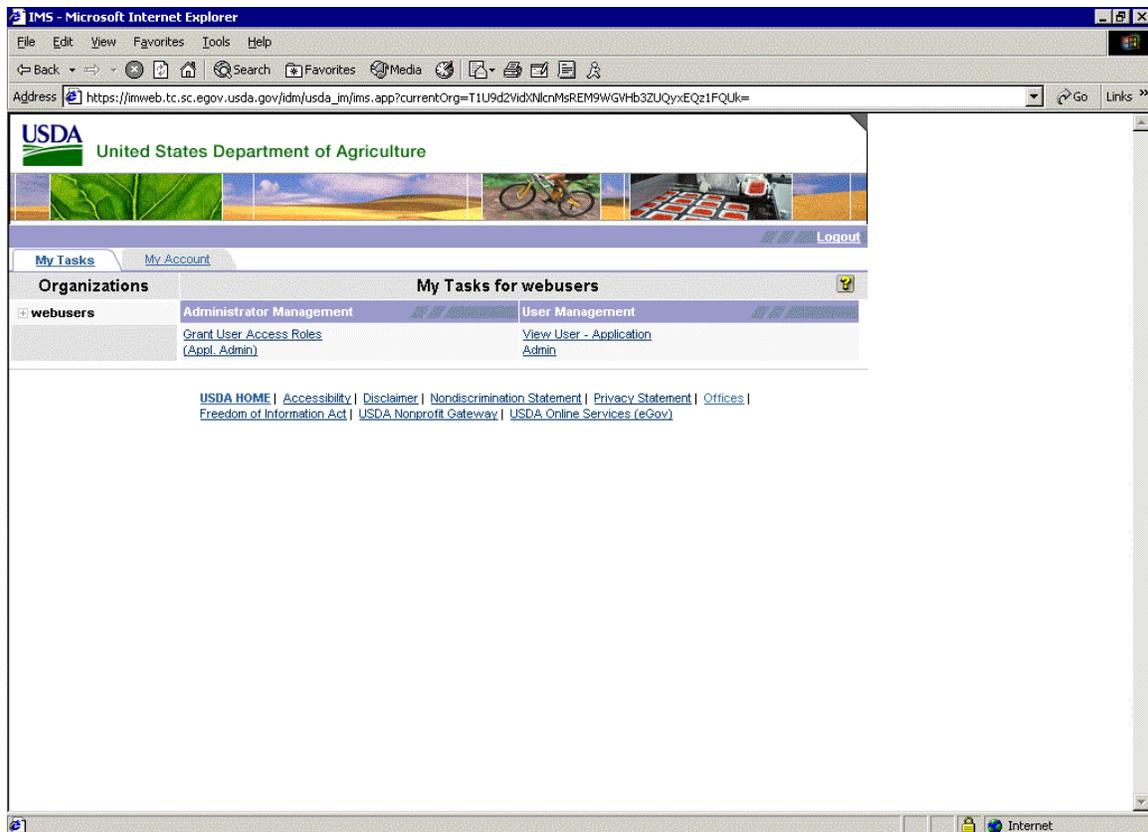
The *Validate Level 2 Customer* page shows the attributes related to the user that is selected. The LRA Administrator enters the specifics of the form of identification used to identity proof the user. In particular they must enter the Credential Document Type and the Credential Expiration for that specific credential.

- If a user clicks on the **Cancel** button at any time, the *Validate Level 2 Customer* page closes.
- If a user clicks the **Submit** button after selecting the Credential Document Type and entering the Credential Expiration, the *Acknowledgement Message* page displays.

3.7.5 Application Administrator

Application Administrators can assign access roles to users. These roles allow users access to specific applications. To perform Application Administrator tasks, authorized users must log in the same way that normal users do. If an Application Administrator clicks the **My Tasks** tab on the **IMS** page, the different organizations for which they may assign Assurance Levels will display. In particular, the organization webusers should appear on the left side of their screen. If the user clicks the **webusers** link, their tasks display.

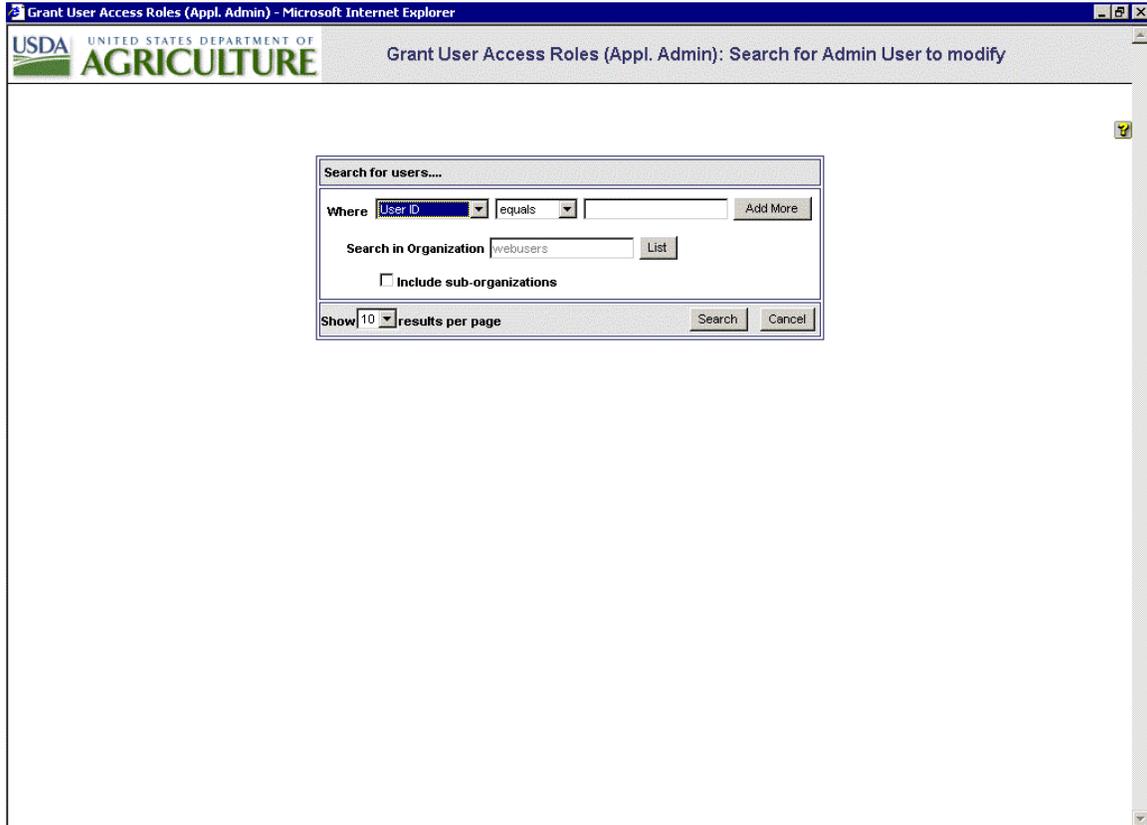
An application Administrator uses the Grant User Access Roles task to assign access roles. This task is seen below on the **IMS** page.



- If a user clicks on the **Grant User Access Role** link, the **Grant User Access Role: Search for a Role Admin User page** displays.

3.7.6 Grant User Access Role: Search for a Role Admin User page

If an Application Administrator clicks the **Grant User Access Role** link on the *IMS* page, the *Grant User Access Role: Search for a Role Admin User* page opens.

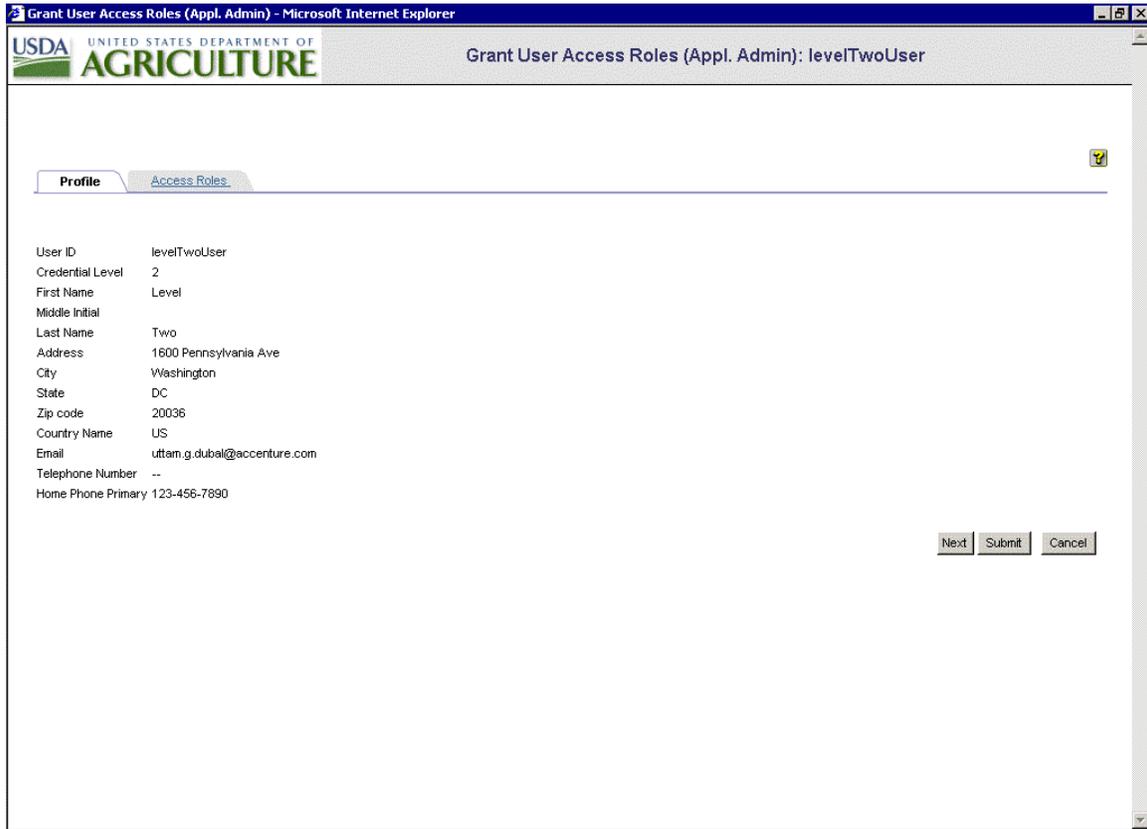


The *Grant User Access Role: Search for a Role Admin User* page allows an Application Administrator to search for a user. The Application Administrator can select a search attribute (Username, Last Name, First Name, or State) from the **Where** drop-down menu. The LRA Administrator can select a comparison attribute (**equals**, **starts with**, **ends with**, or **contains**) from the middle drop-down menu. The Application Administrator enters the text to search for in the text box to the right of the other two fields.

- If a user clicks on the **Search** button, the *Search Results in Organization* page displays. If the user clicks the user in the list on this page the *Grant User Access Roles* page displays.

3.7.7 Grant User Access Roles page

If a user clicks one of the usernames shown on the *Search Results in Organization* page, the *Grant User Access Roles* page displays.



The *Grant User Access Roles* page shows the attributes related to the user that is selected. This is where the Application Administrator is able to grant a user the use of certain application roles.

- If a user clicks on the **Access Roles** tab, the *Access Roles* tab displays.



The *Grant User Access Roles* tab allows Application Administrators to assign users certain access roles. An application administrator can select the **Can Use Role** checkbox to allow the selected user to use the role shown in the same row under Role Name.

- If a user clicks the **Previous** button, they are sent to the last page visited.
- If a user clicks the **Cancel** button at any time, the window will close.
- If a user clicks the **Submit** button, the selected user will be given the rights to use the specific role and an *Acknowledgement Message* page displays.

4 Integration

4.1 Integration Overview

This section describes the processes and tasks involved in the Integration process. The application team will work with the Integration team to progress through the following five (the sixth is optional) major integration stages:

- Pre-Integration stage – This stage includes tasks that must be accomplished before contacting the eAuthentication Integration team.
- Pre-Design Meeting - This stage is the formal beginning of the Integration process, where the application team is introduced to eAuthentication, the primary integrator, and the Integration process itself.
- Design Meeting(s) - This stage is a series of meetings needed to complete the design for the application’s integration.
- Funding - This stage is to assess the agency for the costs to cover integration costs and concludes with the agency’s payment of that bill.
- Build - This stage includes all the technical tasks needed to integrate each of the environments.
- Registration Certification – This stage is only needed for applications that are creating customized registration processes, including non-service center Local Registration Authorities. It includes the design and approval tasks for those processes.

Each of these integration stages along with any underlying tasks is described in detail in the following sections.

4.2 Pre-Integration

Before beginning integration tasks, agencies should complete the tasks included in the pre-integration stage. Once these tasks are complete, the GPEA Implementation team should contact the eAuthentication team at egov@usda.gov to commence integration. The Pre-Integration tasks include:

4.2.1 Form an Application Team

Before performing the pre-integration tasks, agencies will need to identify the key personnel to be involved in the integration effort. This team should be made up of the application development team, application business owners, agency GPEA coordinators, and the agency eAuthentication decision maker.

The eAuthentication Decision Maker is the individual tasked with coordinating all agency integrations.

The GPEA coordinator is the individual in charge of helping the application teams within an agency identify customer facing business functions in the application and report those functions to USDA. The following two sections discuss these tasks.

4.2.2 Integrated Reporting - Identify the Interactions in the Application

Application teams must identify any customer facing interactions within their applications. An interaction is any communication between an application and a customer; for example, the completion of a credit application during a loan application is an interaction, while the entire loan application is called a transaction.

USDA must track which interactions are part of which transactions, as well as which interactions have been put online. This tracking process is called Integrated Reporting. Integrated Reporting tasks include identifying the interactions that the agency will present in an electronic format and establishing whether or not they require eAuthentication. This is done using the Integrated Reporting tool, an online application that facilitates tracking and documenting interactions. The GPEA coordinator for the agency should identify each interaction in the application in the Integrated Reporting Tool, as well as indicate which of those interactions required electronic authentication.

For those interactions where eAuthentication is required, the business owners and agency leads should determine the level of authentication / assurance required, based on the application's risk assessment and their answers to the impact questions in OMB's eAuthentication guidance.

4.2.3 Design and Implement Application

eAuthentication integration must occur concurrently with the rest of the application's software development lifecycle. Before contacting eAuthentication, the application should at least be in a detailed design phase. The application team should have a good idea of the user population submitting data, structure/screen flow of the application, the web addresses to be used, the hosting facilities planned for use (at least the initial environment), and the technology and software being used to develop the application.

4.2.3.1 Consider eAuthentication Platform Compatibility with the eAuthentication agent plug-in should be considered when deciding what application and web server to use.

Some of the more popular web servers and platforms that eAuthentication supports include:

- IIS
- Netscape/iPlanet/SunOne
- Apache
- Stronghold
- IBM HTTP
- Domino
- Oracle HTTP

For a more complete list of the platforms and web servers supported, refer to [Section 5.3.5 eAuthentication Platform Support](#).

4.2.4 Review eAuthentication Guidebook

This guidebook contains a wide range of information about the integration process, ranging from functional overviews, to an overview of online functionality, to technical details. It is continuously updated by the eAuthentication team using their integration experience as well as input from agencies that have already completed the integration process.

Before meeting with the integration team, the application team should read through this document. Likewise, throughout the integration process this document can be used as a reference to answer eAuthentication questions that arise.



4.2.5 Set up Pre-Design meeting with eAuthentication Integration team

After completing all Pre-Integration tasks, the application team should contact the Integration team to set up an integration meeting. This meeting may be requested by calling the eGovernment team at (202) 720-6144 or by emailing the eAuthentication team at eaauth@usda.gov with the subject line “eAuthentication Integration”. An individual’s request should include the following information:

- Their Name
- Their Phone Number
- Their Email Address
- Their work location as well as the Application Team’s location
- Their Application’s Name – both the full name and the acronym

4.3 Pre-Design Meeting

Once all Pre-Integration tasks have been completed, the GPEA implementation team should contact the eAuthentication team to hold the eAuthentication Pre-Design meeting. Attendees at this meeting should include the agency's Application team including the GPEA coordinator, the application development team, the application business owners, and the eAuthentication Decision Maker.

During this Pre-Design meeting members of the integration team will present an overview of the eAuthentication solution, walk through an online demonstration of eAuthentication and explain the integration process including a detailed introduction to the Application Integration Form.

4.3.1 Facilities Needed for the Pre-Design

It is preferable to have the following facilities and equipment for the Pre-Design meeting.

- A meeting room capable of accommodating the application team as well as 2 – 3 integration team members.
- A computer with internet access.
- A computer projector connected to the previous computer.
- A dry erase board.
- A teleconference phone in the event that there are remote parties dialing in.

The meeting can be done with as little as a meeting room, but some of the tasks in the following sections are dependent upon, and enhanced by, the preceding list of equipment.

4.3.2 Introductions to the Integration team

An application team will be assigned a primary integrator. This integrator is responsible for the coordination of work done by the integration team for the application, and will be the primary contact throughout the integration process. The primary integrator will be at the pre-design meeting, and will introduce themselves as well as any other integrators that are attending.

4.3.2.1 How to Contact the Integration team

The integration team may be contacted by either calling the eGovernment phone line at (202) 720-6144 or by emailing the eAuthentication team at eauth@usda.gov. Both of these accounts are monitored by eGovernment personnel and the message and/or call will be forwarded on to the appropriate party.

4.3.3 eAuthentication Overview

The primary task of the pre-design meeting is to present an overview of eAuthentication. This overview includes an explanation the fundamental concepts of eAuthentication as well as a review of the technology, people, and processes/ procedures that make up the eAuthentication solution. The Pre-Design Presentation power point is used to present these topics. The presentation is also available at

http://www.egov.usda.gov/intranet/eauth_docs.html.

To get the username and password to access this site, contact the eGovernment team at eauth@usda.gov.

Many of the concepts explained in the Pre-Design meeting are outlined in this Guidebook. The pre-design presentation should be an opportunity to reinforce the concepts already you have already read about as well as ask any questions that were not answered in this document.

4.3.4 eAuthentication Demonstration

When setting up the location for the Pre-Design meeting, it is preferable to have internet access. If such access is available, the integration team will provide a demonstration of the eAuthentication system. This demonstration will focus on such concepts as:

- eAuthentication Splash/Information Pages
- eAuthentication Account Management
- eAuthentication Self-Registration
- eAuthentication Application Administration

4.3.5 Introduce the Application Integration Form

The Application Integration form is the document that is used to capture the design plans and details required to implement an application's integration. It covers application team contact information, system user information, how an application needs to be protected, technical architecture, firewall and network connectivity issues, integration scheduling and help desk communication plans.

This document is available at http://www.egov.usda.gov/intranet/eauth_docs.html. To get the username and password to access this site contact the eGovernment team at eauth@usda.gov.

4.4 Design Meeting(s)

Following the Pre-Design meeting, the Application team should coordinate a Design Meeting with the primary integrator. The purpose of the Design Meeting(s) is to collect all information needed to completely plan out the application's integration. This information is recorded on the Application Integration form.

The Design Meeting's completion is marked by the completion of the Application Integration form. This step could take multiple meetings. The application team should feel free to contact eAuthentication Integration team as often as necessary.

The following sections outline the major tasks involved in the Design Meeting process:

4.4.1 Choose Hosting Environment(s)

The Application team must finalize their application-hosting model. For integration purposes there are two different hosting categories:

- Hosted in the EAI WebFarms
- Hosted outside the EAI WebFarms

The following two sections describe each of these options as well as the ramifications that each hosting option will have to the integration process.

4.4.1.1 Applications Hosted in the EAI Web Farm

USDA provides a number of hosted facilities for applications. These hosting facilities are located in:

- St. Louis, Missouri
- Kansas City, Missouri
- Fort Collins, Colorado

These facilities together makeup what is referred to as the EAI Web Farm. The EAI Web Farm functions as an Application Service Provider (ASP) by providing a highly available architecture with high-speed access to both the Internet and the USDA Intranet.

The eAuthentication infrastructure is hosted at the Ft. Collins and St. Louis EAI Web Farms. Due to easier access to machines as well as less complicated network connectivity needs, integration complexity is reduced if an application is hosted within that same environment.



4.4.1.1.1 Contacting the Web Farm for Hosting Services

The Web Farm is not affiliated with the eAuthentication service and operates independently. To contact the Web Farm please contact Eric Espedal at (970) 295-5580. Please ensure that the Web Farm is aware that the application will be protected by eAuthentication.

4.4.1.2 Applications Hosted outside the EAI Web Farm

The application team may also host their application at a facility outside the EAI Web Farm. If the application is hosted outside the EAI Web Farms, the following requirements must be met:

4.4.1.2.1 Certification and Accreditation (C&A)

All Applications to be integrated with eAuthentication must have a C&A completed and approved by USDA CyberSecurity. An application can minimize the effort needed to fulfill this requirement if it is hosted within the EAI Web Farm. This is because the web farm network and infrastructure procedures have already undergone C&A compliance requirements.

Contact CyberSecurity regarding C&A for the application to be protected, please contact.

4.4.1.2.2 Compliant Domain Name

If hosted outside of the Web Farm, the application's domain name must end with .usda.gov. This is because the Web server must be on the same domain as the policy server in order for eAuthentication to provide single sign on.

4.4.1.2.3 Firewall Connectivity

The application to be protected must have connectivity to the eAuthentication policy servers in the Fort Collins Web Farm. Agency firewall/network personnel will need to open their firewall to the Fort Collins policy server IP addresses. The integration team will need to open the Fort Collins firewall to the agency server IP addresses. For more information, please refer to Section 4.4.1.2.3: Firewall Connectivity.

4.4.1.2.4 3 Integration Environments

Applications hosted outside the web farm must have a minimum of two environments (Pre-production and Production) dedicated to integration tasks in a similar fashion. Three environments are preferable, which would be comprised of a development, pre-production, and production environment. Each of these environments needs hardware dedicated specifically to that one environment – hosting two environments on the same machine in different virtual directories is not an acceptable solution.

4.4.1.2.5 Administrator Rights

Applications must have an individual assigned to the Application Team that has administrator rights on each web server. These rights need to include the authority to install software, create directories, and set file/folder permissions. This individual should be available to assist with installations and testing.

4.4.2 Determine Application Permission Needs

The Application team should determine how they want each page within their application to be protected. Oftentimes, groups of many different web pages are protected in the same manner. Rather than referring to each of the pages separately, the Application team can refer to groups of pages as “resources”. A resource can be as small as a single web page or large enough to include all the web pages in an application.

An application must identify all the resources that need to be protected in a unique manner, and describe the type of protection that those resources require. All this information is recorded on the Application Integration form.

4.4.2.1 Identifying Resources

To identify the resources, list the URL or folder structure for the files in each resource. If the file is a single page, an example of acceptable identification would be:

www.eauth.usda.gov/application/singlepage.html

If the resource is made up of all the pages within the application folder in the example above, acceptable identification would be:

www.eauth.usda.gov/application/*

4.4.2.2 Types of Protection

Once the Application Permissions required to access each resource have been identified, the application team must describe the type of Application Permission to be applied to each resource. The criteria that can be used to determine Application Permissions include:

- Successfully authenticated users - If a user successfully authenticates then they may access the resource independent of any other criteria.
- The level of assurance allowed access to the resource – indicate whether users with level 1, 2, 3, or 4 can gain access to this resource. Any users with an equal or



higher level of assurance to the one indicated will be able to access the resource. So, if an application indicates level 2, all users with level 2, 3, and 4 credentials will have access.

- Application Permission based upon other user information. This information could be any of the eAuthentication Common Data Attributes that are stored for a user. For instance, it could be set that only users from Illinois can access a particular resource.

4.4.2.3 Determine Role-Based Application Permissions Needs

Protection may also be applied based upon a user's assignment to a particular access role. If an application is using Role-Based Application permissions, a role must be created and named, and attached to each resource that requires such protection.

4.4.2.4 Role Naming Convention

Roles should follow the naming convention:

AgencyAcronym_ApplicationName_RoleDescription

Any role that is specifically intended to identify USDA employees must contain the word "Employee" as a designator. This will aid in later identification of employee users. In the case of an employee the naming convention would be:

AgencyAcronym_ApplicationName_Employee.

The following role descriptions should be used where appropriate:

- User (citizen not designated by any other purpose)
- Govt (Federal government employee other than USDA)
- State (State government employee)
- Farmer (individual farmer)
- Rancher (individual rancher)

The following acronyms should be used for agency role names:

- AMS - Agricultural Marketing Service
- APHIS - Animal and Plant Health Inspection Service
- ARS - Agricultural Research Service
- CNPP - Center for Nutrition Policy and Promotion
- CSREES - Cooperative State Research, Education, and Extension Service
- DA - Departmental Administration & Staff Offices
- ERS - Economic Research Service



- FAS - Foreign Agricultural Service
- FNS - Food and Nutrition Service
- FS - Forest Service
- FSA - Farm Service Agency
- FSIS - Food Safety Inspection Service
- GIPSA - Grain Inspection, Packers and Stockyards Administration
- NRCS - Natural Resources Conservation Service
- NASS - National Agricultural Statistics Service
- RBS - Rural Business-Cooperative Service
- RHS - Rural Housing Service
- RMA - Risk Management Agency
- RUS - Rural Utilities Service

The following examples show acceptable role names:

RHS_Tenant Payments_User

GIPSA_Quality Products_Rancher

ERS_ARMS_Employee

4.4.3 Determine Authorization Needs

Authorization is different from authentication. Authentication is the verification that a person or thing is who they say they are. Authorization is the verification that the person or object has permission to do perform a function. Authorization is performed internally within an application. While eAuthentication can supply information that helps an application perform Authorization, the actual functionality must be created by the application.

If the application needs to perform Authorization, eAuthentication can facilitate this effort by sending USDA Common Data. eAuthentication can send any of the information that it stores to particular resources within an application. The application team must identify the resources that need to receive this USDA Common Data, and which USDA Common Data attributes each resource needs to receive.

4.4.3.1 USDA Common Data and Header Variables

To facilitate any authorization needs, an application can receive any information stored as eAuthentication Common Data. Once a user signs on and accesses a particular resource, eAuthentication polls its USDA Common Data store. Any user data that is specified to be sent to that resource is placed in a Header Variable and sent to the web or application server.

This information is sent to the application as an encrypted server-side, header variable. Each header normally consists of a single line of ASCII text with a name and a value.



Such header variables must be read on a server using server-side technology (ASP, JSP, etc.).

The schema for USDA Common Data is set. Data that is collected and required (or not required) cannot be changed per application needs. Attributes required and collected differently for users' accounts with different assurance levels. If an agency would like additional information about the user, they must collect, store, and manage that information within their application's data store.

For more information on the data stored or how to reference the data, refer to Section 4.6.4: Understanding and Capturing Header Variables.

4.4.4 Design the Mapping Process Application Users to the eAuthentication Common Data Store

Users will be authenticated with eAuthentication services. If any additional user data is being stored by the application, user's eAuthentication unique key will need to be matched to the user's unique key in the local database. This matching process is called data mapping. eAuthentication uses a unique key is called the "USDA eAuth Internal ID."

Most often, agencies will be required to add the USDA eAuth Internal ID column to their databases and associate that USDA eAuth Internal ID with the appropriate person in their data store. Once this is complete, applications can look up the user in their data store using the USDA eAuth Internal ID.

4.4.5 Design Logoff page

A session cookie is created when a user first signs on and is authenticated by eAuthentication. This session cookie allows the user to view different resources without the need to sign on again. When a user needs to end their session, they must go to a page that is designated by eAuthentication as a logoff page. The logoff page deletes the session cookie, so that the next time the user attempts to access a protected resource they are prompted for their User ID and Password.

Applications need to create links that send their users to a logoff page. Different strategies can be used to facilitate these logoff pages. These strategies are outlined in the following sections.

4.4.5.1 Global Logoff Page

eAuthentication has a centralized logoff page that is hosted with the rest of the system. This page accomplishes two functions:

- It ends the eAuthentication single-sign on session for the user browsing the page, by deleting the session cookie. The next time that user attempts to access a protected resource, they are prompted for their User ID and Password.
- It redirects users back to a link as specified by the application from which the user was sent. By doing this, an application team can custom tailor their user experience, sending that user to a splash page, a USDA hosted page, back to the log on page, etc.

The use of the centralized logoff page serves as the default for eAuthentication implementation.

4.4.5.2 Local Logoff Page

Local logoff page functionality is supported by installing and designating a logoff URL on each application's web server. When a user clicks on the page, the web agent installed on the web server deletes the session cookie for the user currently authenticated (i.e. currently logged-in). The next time that user attempts to access a web site protected by eAuthentication, he/she is prompted for their credentials.

Application owners are responsible for developing the html for the local logoff page. Integrators are responsible for implementing the logoff functionality that ends the user's eAuthentication session.

A Local Logoff page must be hosted on the web server containing an application's web agent. It must be hosted inside a domain protected by eAuthentication on that web server. For testing purposes, it is easiest if installation of the logoff page is done during a web agent install. It can however be added at any time in the integration process.

4.4.5.3 Application Only Logoff Functionality

The link to the application only logoff page may contain a trigger for functionality that closes the user's application session, rather than their eAuthentication session (if such a session exists). That user could continue to benefit from single sign on capabilities. This application functionality must be implemented by the application team, not the integration team. Likewise, it is entirely at the application team's discretion as to if and how this functionality is implemented.



4.5 Funding

Once the Design Meeting(s) have been completed, a bill is created and sent to the agency. This bill will pay for the cost of integration with eAuthentication. No further integration tasks can proceed until funding is approved and a payment is made.

Funding costs are based on a general funding model, which in turn is based on the information contained in the completed application integration form. This funding model was approved by the USDA eGovernment decision makers on February 2, 2004.

4.5.1 How is funding determined?

The billing amount for the integration is calculated using the details resulting from the Design Meeting(s) and recorded on the application integration form. A standard valuation is assigned to each of the major integration factors, such as hosting location and types of application permission and authorization needed, according to the level of integration effort each factor entails.

4.5.2 Who makes the decision?

A funding cost for each application is determined by the eAuthentication Project Manager. This individual conveys the billing amount to the agency's CIO and eAuthentication Decision Maker, who must approve the amount before an invoice is created and a payment is made.

4.6 Build

The build phase consists of the steps needed to actually integrate an application. Build tasks must be completed in each of the environments that an application is planning to use. During this time, the agency may schedule Build Coordination meetings with the eAuthentication team as needed. Test meetings may also be scheduled with the eAuthentication team once the web agent is installed and the application is integrated. These meetings are completely optional and may also include teleconferences.

The three environments used in the build phase are:

Development – used to code integration

Pre-Production – used to test performance of the integration

Production – used to host the live application

Certain integration tasks must be completed before completing integration in one environment and moving it to the next environment. Those integration tasks include the following:

4.6.1 Network Connectivity between the Policy Server and the Web Agent

A secure connection must be established between the eAuthentication primary policy server in the Ft. Collins Web Farm and the application's web server. This connection allows the web agent to communicate with the policy server. All policy servers reside behind a firewall which must be configured to allow traffic from the web server. The policy server(s) for each of the three environments resides behind a different firewall. The integration team will configure the Fort Collins firewall to allow traffic from each of an application's web servers. To do this they will need the IP address for each server that is being used. This information is recorded on the Application Integration form.

An application team needs to make sure that their web server can receive traffic from the eAuthentication policy servers. If application's web server is located behind a firewall, the firewall must be configured to allow bi-directional traffic to the IP address of the corresponding policy server (development server to development policy server, etc.). This traffic must be open over the following ports (the information being sent across each port is also listed):

- 44441 - Accounting service
- 44442 - Authentication service
- 44443 - Authorization service
- 44444 - Administration service

4.6.2 Install Web Agents

The integration team must install a piece of software called a web agent on each machine hosting the application. The primary integrator will likely travel to the server’s hosting site to install this software. An individual with administration rights to the machine will need to assist with the process. Network connectivity should be established before the installation begins.

4.6.2.1 Log Files

The web agent generates log files that allow the integration team to troubleshoot any issues with the web agent. The directory in which will be used to store the web agent log files must be identified in advance of the web agent installation.

4.6.3 Configure Integration

The integration team will configure the policy server to contain all Application Permission and Authorization rules as specified by the Application Integration form. This task is performed entirely by the Integration team.

4.6.4 Understanding and Capturing Header Variables

4.6.4.1 SiteMinder Default Header Variables

The following list of attributes contains system attributes that are always passed to any protected resource (those header variables that are not needed may be ignored):

Default eAuthentication Header Variables

Default HTTP Header	Description
HTTP_SM_AUTHDIRNAME	The name of the directory against which the Policy Server authenticates the user. The administrator specifies this directory in the SiteMinder User Directory dialog box in the Policy Server User Interface.
HTTP_SM_AUTHDIRNAMESPACE	The directory namespace against which the Policy Server authenticates the user. The administrator specifies this namespace in the SiteMinder User Directory dialog box in the Policy Server User Interface.
HTTP_SM_AUTHDIROID	Directory object identifier (OID) from the Policy Server database.



Default HTTP Header	Description
HTTP_SM_AUTHDIRSERVER	The directory server against which the Policy Server authenticates the user. The administrator specifies this directory server in the SiteMinder User Directory dialog box in the Policy Server User Interface.
HTTP_SM_AUTHENTIC	Authentication status of the user. Confirms that the user is authenticated. The Agent includes this header only if the user is authenticated. If the user is not, this header is not returned. This header is also not returned if the resource is unprotected.
HTTP_SM_AUTHORIZED	Confirms that the user is authorized. The Agent includes this header only if the user is authorized. If the user is not, this header is not returned. This header is also not returned if the resource is unprotected.
HTTP_SM_AUTHREASON	The code the Web Agent returns to the user after a failed authentication attempt or secondary authentication challenge.
HTTP_SM_AUTHTYPE	Type of authentication scheme the Policy Server uses to verify the user's identity.
HTTP_SM_DOMINODATA	This header is for SiteMinder internal use only that stores the client IP address.
HTTP_SM_REALM	SiteMinder realm in which the resource exists.
HTTP_SM_REALMOID	Realm object ID that identifies the realm where the resource exists. This ID is may be used by third party applications to make calls to the Policy Server.
HTTP_SM_SDOMAIN	Agent's local cookie domain.
HTTP_SM_SERVERIDENTITYSPEC	Policy Server identity ticket, which keeps track of the user identity. The Web Agent uses this to access content protected by anonymous authentication schemes so it can personalize the content for the user.
HTTP_SM_SERVERSESSIONID	A unique string identifying a user session.



Default HTTP Header	Description
HTTP_SM_SERVERSESSIONSPEC	Ticket that contains user session information. Only the Policy Server knows how to decode this information.
HTTP_SM_TIMETOEXPIRE	Amount of time remaining for a SiteMinder session.
HTTP_SM_TRANSACTIONID	Agent-generated unique ID for each user request.
HTTP_SM_UNIVERSALID	Policy Server-generated universal user ID. This ID is specific to the customer and identifies the user to the application, but it is not the same as the user login.
HTTP_SM_USER	Login name of the authenticated user.
HTTP_SM_USERDN	The user's distinguished name recognized by SiteMinder.
HTTP_SM_USERMSG	The text that the Agent presents to the user after an authentication attempt. Some authentication schemes supply challenge text or a reason why an authentication has failed.



4.6.4.2 USDA Common Data Header Variables

The following list of user attributes will be collected upon registration and stored in the eAuthentication centralized database. An agency can choose to have some of these attributes passed as header variables in addition to the default header variables to be passed to any of its resources for authorization purposes.

USDA Common Data

Table with 5 columns: Attribute Name, Description, Header Variable Name, Type, Required/Registration Level. Rows include attributes like USDA eAuth Internal ID, Credential Level, AccountCreationDate, etc.

The fields contained on this table are defined as follows:

- Attribute Name - Contains the title of the attribute for each header variable.
• Description - Contains details about each particular attribute.
• Header Variable Name - Contains the string that will be passed to each application in actual header variable.

usda_last_name = smith (Where the user's last name is Smith).

- Type - Contains the data type of each variable that is passed.



- **Required / Registration Level** – Describes whether the information is required or not per a particular Assurance/Registration level.
 - Not required - an attribute that can be entered at both level 1 and 2, but is never required.
 - System Entered at Level 1 - an attribute that is automatically assigned to a user at level 1.
 - Required at Level 1 - an attribute that a user is required to enter to register for a level 1 account
 - Required at Level 2 - an attribute that a user is required to enter to register for a level 2 account. This should be taken into account when an agency decides which fields they will depend on to provide customization and authorization.

4.6.4.3 Reading Header Variables in ASP

When reading SiteMinder header variables in ASP, they must be parsed from the ALL_HTTP variable. The following ASP code contains the function necessary to parse for the SiteMinder header variables.

```
<%  
Function GetAttribute(AttrName)  
    Dim AllAttrs  
    Dim RealAttrName  
    Dim Location  
    Dim Result  
  
    AllAttrs = Request.ServerVariables("ALL_HTTP")  
    RealAttrName = AttrName  
    Location = instr(AllAttrs, RealAttrName & ":")  
  
    if Location <= 0 then  
        GetAttribute = ""  
        Exit Function  
    end if  
  
    Result = mid(AllAttrs, Location + Len(RealAttrName) + 1)  
    Location = instr(Result, chr(10))  
  
    if Location <= 0 then Location = len(Result) + 1  
        GetAttribute = left(Result, Location - 1)  
  
End Function  
  
Dim Username = GetAttribute("HTTP_SM_USER")
```



%>

Below is a sample ASP code to test if user has been authenticated through SiteMinder. If the user has not yet been authenticated, the header variable will not have a value. If the user has been authenticated, the username will be in the header variable and the asp code can assign the value to a declared string.

```
<% @ Language=VBScript %>
<%
    Dim strUserName

    'If user has been authenticated, get the name from SiteMinder.
    If Not ((IsEmpty(getAttribute("HTTP_SM_USER"))) and _
    (getAttribute("HTTP_SM_USER")<>"")) Then

        'Record the UserName from SiteMinder
        strUserName = Request.ServerVariables("HTTP_SM_USER")

        --- Extend this asp as needed to continue ---
    %>
```

*note: this code uses the `getAttribute()` function defined above

4.6.4.4 Reading Role Names in ASP

Role names are passed in a manner similar to Header Variables. All of a user's roles are passed to the application in a particular header variable. The application can search through that header variable for a particular role.

The following function contains an example of the code needed to do this. The function `roleExists` takes in a role to search for in the format of a string. It will return "true" if the role is being returned by SiteMinder and "false" if the role is not present.

```
<%
function roleExists( searchRole )
    dim userRoles
    dim result

    userRoles = getAttribute( "HTTP_USDAROLES" )
    result = inStr( userRoles, searchRole )

    if result = 0 then
        roleExists = false
    else
        roleExists = true
    end if
end function
```



end if

End Function

%>

An example of how the call would be made from a web page is as follows:

```
<html>
<head>
<title>Role Exists</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>
<body>
<%
if roleExists( "ROLENAME" ) = true then
  Response.write("Exists")
else
  Response.write("Does not exist")
end if
%>
</body>
</html>
```

4.6.5 Build Data Mapping Page(s)

Users will be authenticated with eAuthentication services. If data is being stored by the application, the user's eAuthentication unique key will need to be matched to the user's unique key in the local database. This matching process is called data mapping. eAuthentication's unique key is called the USDA eAuth Internal ID.

Most often, agencies will be required to add the USDA eAuth Internal ID column to their databases and associate that USDA eAuth Internal ID with the appropriate person in their data store. Once this is complete, Applications can look up the user in their data store using that USDA eAuth Internal ID.



4.6.6 Build Logoff Page

The logoff functionality for Local and Global logoff pages is implemented by the Integration team. The application team will still need to accomplish several tasks depending upon the type of logout page that is implemented.

4.6.6.1 Global Logoff Page

If a Global logoff page is used, the application is required to specify a redirect address to be used, if any. This URL should be included in the query string of any links contained in the application that point to the Global Logoff page.

To specify a page for redirect, an application will provide the URL of that page in an HTTP query string appended to the link pointing to the Global Logoff page. The Global Logoff page will read that query string, scrape the URL and use it to process the redirection.

The query string contains a variable/value pair in the format of:
AGENCYTARGET = “redirection URL”

The Global Logoff page URL is

<https://pws.sc.egov.usda.gov/siteminderagent/dmsforms/logoff.asp>?. If an application wanted to redirect to <http://www.usda.gov> then the link to the logoff page would contain the following link and query string to specify the redirect page:

<https://pws.sc.egov.usda.gov/siteminderagent/dmsforms/logoff.asp?AGENCYTARGET=http://www.usda.gov>

If no URL page is specified in the query string of the link, the logoff page will send the user to a default redirect page.

4.6.6.2 Local Logoff Page

If the application is using a Local Logoff page, all that the application team is responsible for is designing the html page that will be used for the logoff. The integration team will implement the logoff functionality using the URL that is specified. It is important to remember that there can only be a single logoff page per web server, even if multiple applications protected by eAuthentication are hosted on that server.

4.6.7 Test Integration

Once the web agent has been installed and eAuthentication has been configured, the application team and the integration team must test the integration. This confirms that the



integration has been configured and performed correctly, and must be completed before moving on to the next environment.

To facilitate this testing process, the integration team will provide the application team with an Integration Test form. This form outlines all the parts of the integration that need to be tested. Also included on this form are a variety of mockup users that can be used for all needed test purposes.

4.6.7.1 Setup Test Machine Firewall Connectivity

Because the development and pre-production environments are hosted behind the Web Farm firewall, the application team needs to identify the IP addresses or ranges of any client machines that will be used for test purposes.

4.6.7.2 Why Signoff is Important

Once testing is complete and the application team has verified that the integration is functioning properly, the completed test form should be returned to the integration team. This completed form is considered signoff from the application team. It signifies that the environment is operating correctly and that the application team is ready to proceed with the migration to the next environment. Having this sign-off ensures that everything is working correctly. Without it, the integrator cannot further migrate the application.

4.6.8 Migrate to Production

Once all build tasks have been completed for the development and/or pre-production environments, the application is ready to be migrated to production. This migration request will be submitted to the eAuthentication Operations team by the primary integrator. The Operations and Integration team will work together to perform the migration configuration as well as assist with the web agent installation on the production server.

Migration of an application to production occurs prior to the application's go-live date (this is the date that the application is released and advertised to the public). Once an application has been migrated to production, the team should be prepared to test that the integration was performed correctly.

4.7 Registration Certification

While the Application Development team is working on the technical build, the GPEA implementation team should determine whether or not additional user registration processes are needed. If they are needed, the team should proceed with the certification process. This integration step is optional and is only needed for applications requiring level 2 assurance and whose users cannot make use of service centers for their registration needs.

A USDA agency can choose to train certain employees to act as LRA's to facilitate their applications' identity proofing needs. This training is offered online. To get access to this training contact your primary integrator and have the names and User ID's of the employees that you would like to train as LRA's ready. It is important that all users register for level 2 eAuthentication accounts prior to requesting this training.

5 Detailed Development Information

5.1 Password Policies

eAuthentication users are responsible for setting and managing their level 1 or 2 passwords. This section outlines the standards and requirements that define Password Management procedures.

5.1.1 Password Policy Level One

The password policy for level one that will be implemented as part of the eAuthentication solution is as follows:

- Passwords must be between 4 and 10 characters long.
- Passwords must contain the following:
 - At least 1 uppercase letter
 - At least 1 numerical digit
- Passwords CANNOT contain the user's first name, last name, or User ID.

5.1.2 Password Policy Level Two

The password policy for level two that will be implemented as part of the eAuthentication solution is as follows:

- Passwords must be between 8 and 14 characters long.
- Passwords must contain the following:
 - At least 1 uppercase letter
 - At least 1 lowercase letter
 - At least 1 numerical digit
 - At least 1 of the following special characters:
 - ! @ # - \$ % * = + : ; , ? ~
- Passwords CANNOT contain the user's name first or last or User ID.
- Passwords CANNOT contain dictionary words, spaces, tabs, or any other special characters not listed above.

5.1.3 Force Change Password

5.1.3.1 Temporary Passwords

Users will be forced to change their password any time they login with an eAuthentication-produced (temporary) password. This will include users logging in for



the first time using pre-populated account information and users logging in using temporary passwords after using the forgotten password functionality.

5.1.3.2 User-prompted change

Users may change their password online at any time.

5.1.3.3 Password Expiration/Lifetime

User passwords expire after a certain period of time. Upon expiration, the user will be prompted to change their password before being allowed to login.

5.2 Account Policies/Session Management

5.2.1 Account Expiration

Unused accounts will be automatically deactivated after 13 months without use. If a user attempts to access a deactivated account, they will be instructed to call the eAuthentication Help Desk for account reactivation.

5.2.2 Account Lockout

A user will be locked out of their account after three unsuccessful login attempts. The lockout will last for a certain period of time before the user can attempt to login again. This period of time is 60 seconds for level 1 users and 60 minutes for level 2 users.

5.2.3 Maximum Timeout

By setting a maximum timeout, a user must re-login after certain period of time regardless of user activity. If a user tries to access a protected resource after the maximum timeout period has elapsed, SiteMinder will redirect the user to the login screen and force the user to re-login. Once logged in, the user will be taken back to the resource he/she tried to access before timeout. The maximum timeout setting for eAuthentication is 9 hours.

5.2.4 Idle Timeout

If the idle-timeout parameter is configured, a user must re-login after certain period of inactive time. For example, if the idle timeout is set to 15 minutes, and user leaves the desk for 20 minutes, the user will be forced to login again when he/she tries to access a protected resource. The idle timeout setting that will be implemented as part of the eAuthentication solution is 2 hours.

5.3 Netegrity SiteMinder References

In order to protect resources in SiteMinder, the eAuthentication team must create a Policy Domain which contains Realms, Rules, Responses, and Policies. The integration survey that agencies fill out during the planning phase will allow eAuthentication team members to create these SiteMinder policies.

Descriptions of the components of SiteMinder policies as well as examples of each are given below.

5.3.1 Realms

A Realm is a group of resources within a policy domain defined according to security requirements. A Realm can be everything under a whole web server (example – http://agency1.usda.gov/*), or it could be sub-directories under a web server (example – http://agency1.usda.gov/app1/* or http://agency1.usda.gov/app2/images/*). Once a Realm is created, the resources under the realm can be protected.

5.3.2 Rules

A Rule must be associated with a Realm. Rules can be set to protect individual files (like <http://agency1.usda.gov/index.html>) or groups of files (http://agency1.usda.gov/*.pdf) and either allow or deny access to the resources. Rules can trigger responses during authentication and authorization events as well. A user can also apply granular time control to access protected resources. For example, a setting may allow users to access agency1 application only from 7:00am to 7:00pm; Monday through Friday. A rule may also restrict access to an application based on a physical location, such as an IP address.

5.3.3 Responses

A Response can be used to perform certain actions depending on the events. For example, if a user does not have the rights to access resource.html, a response can redirect the user to an html page that indicates that the user does not have the rights to access the resource. A response can also return profile information from the enterprise directory (e.g. a user's role and/or phone number). Responses are associated with rules.

The SiteMinder Administrator can configure response triggered by the following events:

- Authentication Events
- Authorization Events
- Web Agent Actions
- Policies

5.3.3.1 Authentication Events

The Policy server can trigger an authentication event based on the outcome of the authentication. The Authentication events include:

- OnAuthAccept – This event will be triggered when authentication is successful.
- OnAuthReject – This event will be triggered when authentication is failed.
- OnAuthChallenge – This event will be triggered when user is challenged with authentication.
- OnAuthAttempt- This event will be triggered when user while attempting to authenticate.

5.3.3.2 Authorization Events

The Policy server can trigger an authorization event based on the outcome of the authorization. The authorization events include:

- OnAccessAccept – This event will be triggered when user is successfully authorized.
- OnAccessReject – This event will be triggered when user is not authorized.

5.3.3.3 Web Agent Actions

The Policy Server allows the responses to be triggered by http methods, GET, POST, and PUT.

5.3.3.4 Policies

Policies are used to associate groups of users to rules, and responses to rules. A user can also associate time restriction, IP address, and Active Policy with the policy. For example, a Policy can grant “agency1” users access to a resource 24 hours a day, and return the username name to the portal for personalization.



5.4 eAuthentication Platform Support

The platforms supported by eAuthentication are constantly expanding. To get the latest update please contact your primary integrator or send an email to eAuth@usda.gov.

	NT/W2K*	WIN 2003	SOLARIS 8, 9	HPUX ¹⁰ 11.0, 11i	AIX? 4.3.3, 5.1	RED HAT LINUX
WEB AGENT						
Microsoft IIS						
☞ V4, 5	Yes					
☞ V6.0		Yes ⁹				
SunOne						
☞ V4.1, 6.0	Yes		Yes	Yes	Yes ¹	
Apache						
☞ V 1.3.27			Yes ^{RP}	Yes ^{RP}		Intel Only 7.2 ^{2,3} , 7.3 ^{2,3} Yes ^{RP}
☞ V 2.0.43 ⁵	Yes ^{RP}		Yes ^{RP}	Yes ^{RP}		Intel Only 7.2 ^{2,3} , 7.3 ^{2,3} Yes ^{RP}
Stronghold V3						
☞ Apache 1.3.22 (3017)			Yes ^{RP}	Yes ^{RP}		
Stronghold V4						
☞ Apache			Yes ^{RP}	Yes ^{RP}		
Covalent Apache						
☞ FastStart 2.1 (Apache 1.3 based)			Yes			
☞ Enterprise Ready Server 2.3 (Apache 2.0.43 based)			Yes			Intel Only 7.2, 7.3 Yes
IBM HTTP Server						
☞ 1.3.19.4			Yes		Yes	
☞ 1.3.26.1			Yes		Yes	
☞ 2.0.42.1			Yes			
☞ 2.0.42.2						
Domino						
☞ V5.0.10	Yes		Yes			



	NT/W2K*	WIN 2003	SOLARIS 8, 9	HPUX ¹⁰ 11.0, 11i	AIX? 4.3.3, 5.1	RED HAT LINUX
WEB AGENT						
⚡ V5.0.12	No		No			
⚡ V6.0.2	No		No			
Oracle HTTP Server						
⚡ V 9.0.2			Yes	Yes		
⚡ V 9.0.3			No	No		
HP Apache Server						
⚡ V 2.0				No		
Application Server Agent						
WebSphere						
⚡ V 4.0	Yes		Yes ⁶	Yes ⁸	Yes ⁷	
⚡ V 5.0	Yes		Yes ⁶		Yes ⁷	

Legend:

* = Windows NT 4.0 SP 6a Server and Windows 2000 SP4 Server/Advanced Server

Yes = currently supported for SiteMinder v5.0 forward

RP = Reverse Proxy is supported. If this is not listed above on a web server that supports reverse proxy, this configuration is not supported with the Agent.

Notes:

1. iPlanet 6.0 is supported on AIX.
2. Supports Apache with SSL.
3. Apache version bundled with RedHat not supported. Please install ?regular? Apache web server on RedHat.
5. Apache 2.0 does not support eTelligent Rules.
6. Solaris 8 only.
7. AIX 5.1 only.
8. HPUX 11i only.
9. Starting from 5QMR5 Hotfix 004.
10. Agents are only supported on HPUX 11/0 operating System. Web agents on HPUX do not support PA-RISC 1.x.